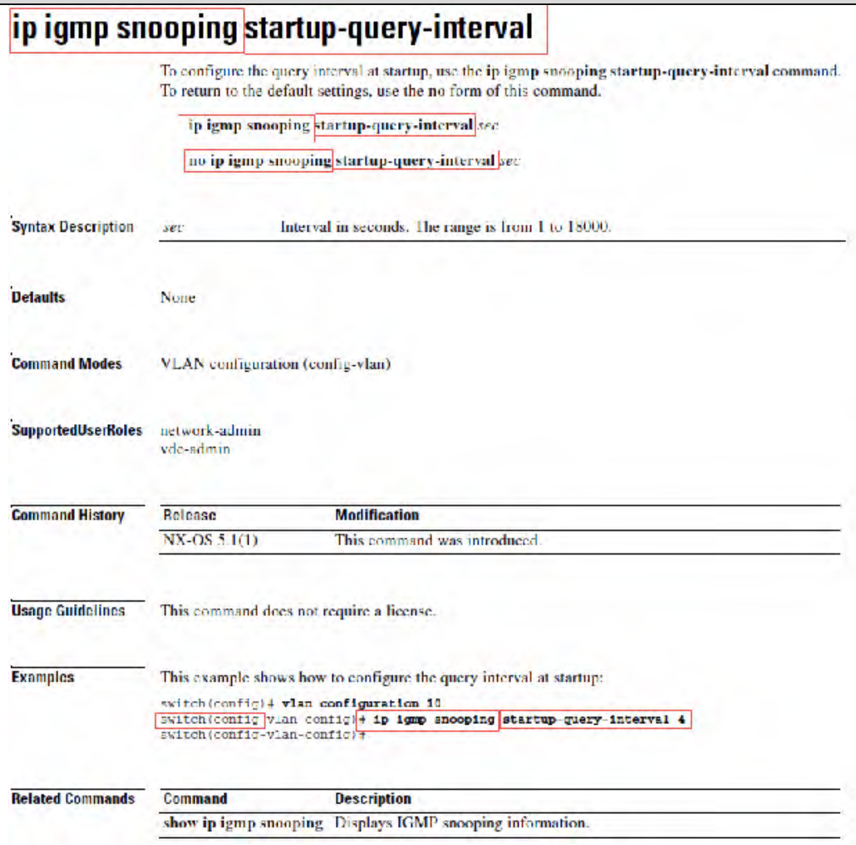
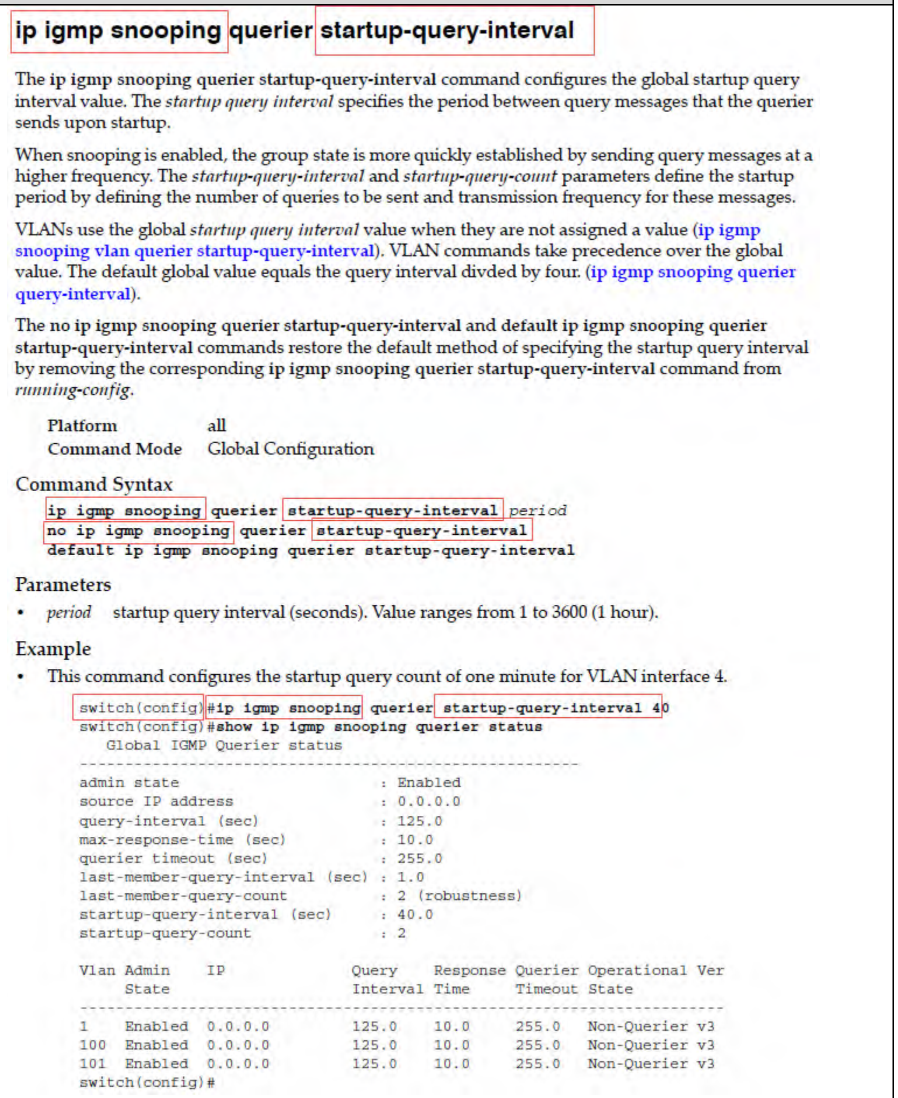
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 105.	 Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1813.

ip igmp snooping startup-query-interval

To configure the query interval at startup, use the **ip igmp snooping startup-query-interval** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping startup-query-interval *sec*

no ip igmp snooping startup-query-interval *sec*

Syntax Description

sec	Interval in seconds. The range is from 1 to 18000.

Defaults None

Command Modes VLAN configuration (config-vlan)

SupportedUserRoles network-admin
vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to configure the query interval at startup:

```
switch(config)# vlan configuration 10
switch(config-vlan-config)# ip igmp snooping startup-query-interval 4
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping querier startup-query-interval

The ip igmp snooping querier startup-query-interval command configures the global startup query interval value. The *startup query interval* specifies the period between query messages that the querier sends upon startup.

When snooping is enabled, the group state is more quickly established by sending query messages at a higher frequency. The *startup-query-interval* and *startup-query-count* parameters define the startup period by defining the number of queries to be sent and transmission frequency for these messages.

VLANs use the global *startup query interval* value when they are not assigned a value (ip igmp snooping vlan querier startup-query-interval). VLAN commands take precedence over the global value. The default global value equals the query interval divded by four. (ip igmp snooping querier query-interval).

The no ip igmp snooping querier startup-query-interval and default ip igmp snooping querier startup-query-interval commands restore the default method of specifying the startup query interval by removing the corresponding ip igmp snooping querier startup-query-interval command from *running-config*.

Platform	all
Command Mode	Global Configuration

Command Syntax

```
ip igmp snooping querier startup-query-interval period
no ip igmp snooping querier startup-query-interval
default ip igmp snooping querier startup-query-interval
```

Parameters

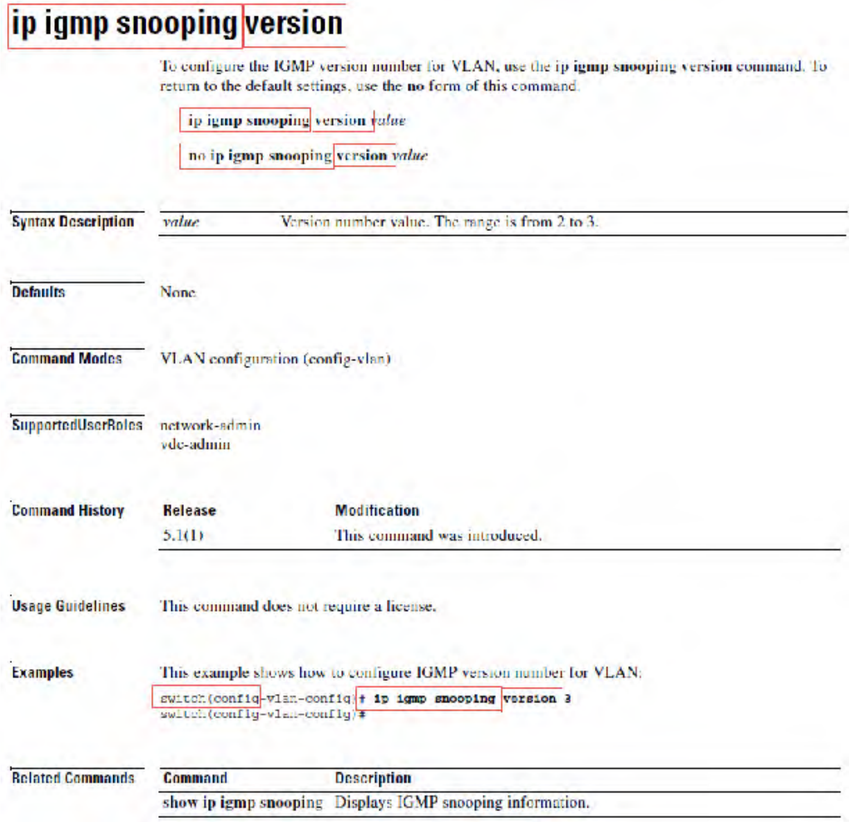
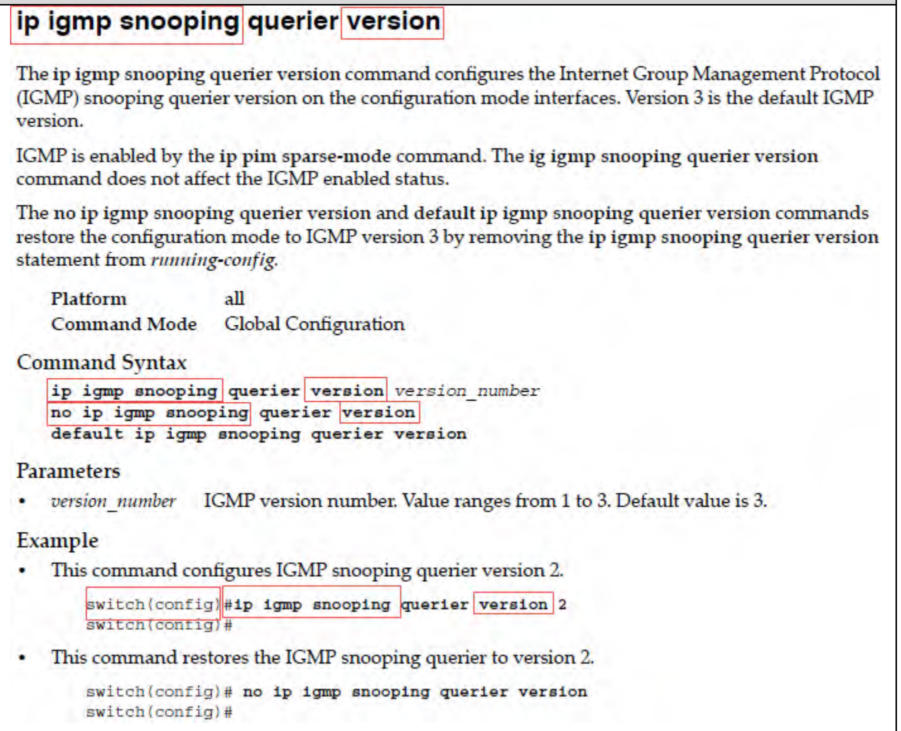
- *period* startup query interval (seconds). Value ranges from 1 to 3600 (1 hour).

Example

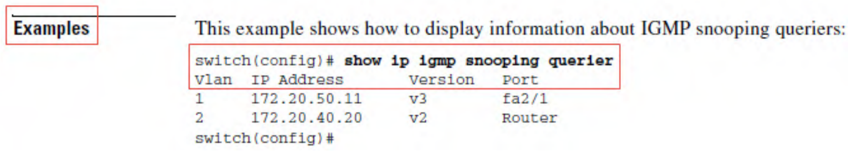
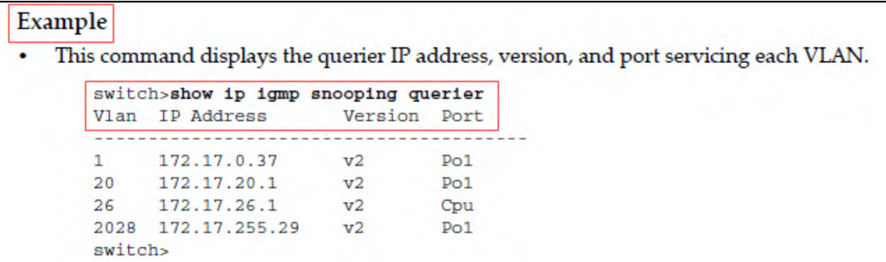
- This command configures the startup query count of one minute for VLAN interface 4.

```
switch(config)#ip igmp snooping querier startup-query-interval 40
switch(config)#show ip igmp snooping querier status
   Global IGMP Querier status
--------------------------------------------------------------
admin state                           : Enabled
source IP address                     : 0.0.0.0
query-interval (sec)                  : 125.0
max-response-time (sec)               : 10.0
querier timeout (sec)                 : 255.0
last-member-query-interval (sec)      : 1.0
last-member-query-count               : 2 (robustness)
startup-query-interval (sec)          : 40.0
startup-query-count                   : 2

Vlan Admin    IP                  Query    Response Querier Operational Ver
     State                        Interval Time     Timeout State
-------------------------------------------------------------------------
1    Enabled  0.0.0.0             125.0    10.0     255.0   Non-Querier v3
100  Enabled  0.0.0.0             125.0    10.0     255.0   Non-Querier v3
101  Enabled  0.0.0.0             125.0    10.0     255.0   Non-Querier v3
switch(config)#
```

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	ip igmp snooping version
	To configure the IGMP version number for VLAN, use the ip **igmp snooping version** command. To return to the default settings, use the **no** form of this command.
	ip **igmp snooping version** *value*
	no ip **igmp snooping version** *value*
	Syntax Description — *value* — Version number value. The range is from 2 to 3.
	Defaults — None.
	Command Modes — VLAN configurstion (config-vlan)
	SupportedUserRoles — network-admin
	vde-admin
	Command History — **Release** — **Modification**
	5.1(1) — This command was introduced.
	Usage Guidelines — This command does not require a license.
	Examples — This example shows how to configure IGMP version number for VLAN:
	`switch(config-vlan-config)# ip igmp snooping version 3`
	`switch(config-vlan-config)#`
	Related Commands — **Command** — **Description**
	show ip igmp snooping — Displays IGMP snooping information.
	Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 108.
		
		ip igmp snooping querier version
		The **ip igmp snooping querier version** command configures the Internet Group Management Protocol (IGMP) snooping querier version on the configuration mode interfaces. Version 3 is the default IGMP version.
		IGMP is enabled by the **ip pim sparse-mode** command. The **ig igmp snooping querier version** command does not affect the IGMP enabled status.
		The **no ip igmp snooping querier version** and **default ip igmp snooping querier version** commands restore the configuration mode to IGMP version 3 by removing the **ip igmp snooping querier version** statement from *running-config*.
		Platform all
		Command Mode Global Configuration
		Command Syntax
		`ip igmp snooping querier version version_number`
		`no ip igmp snooping querier version`
		`default ip igmp snooping querier version`
		Parameters
		• *version_number* IGMP version number. Value ranges from 1 to 3. Default value is 3.
		Example
		• This command configures IGMP snooping querier version 2.
		`switch(config)#ip igmp snooping querier version 2`
		`switch(config)#`
		• This command restores the IGMP snooping querier to version 2.
		`switch(config)# no ip igmp snooping querier version`
		`switch(config)#`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1815.

Copyright Registration Information	**Cisco**	**Arista**

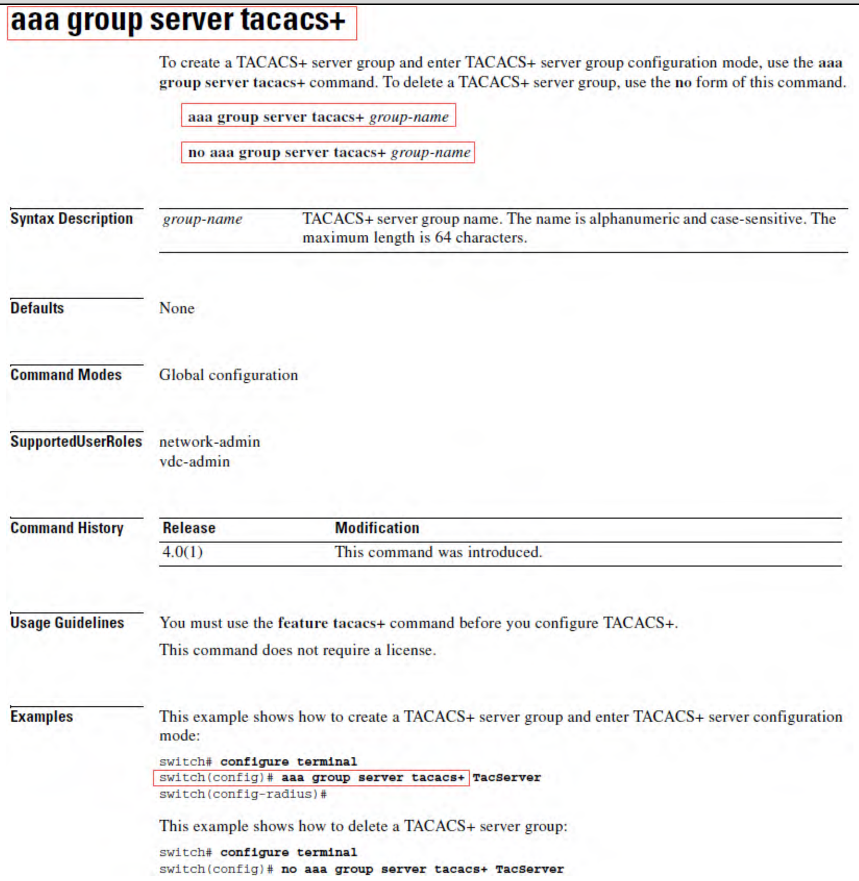
Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	Examples
	This example shows how to display information about IGMP snooping queriers:
	`switch(config)# show ip igmp snooping querier`
	`Vlan  IP Address      Version    Port`
	`1     172.20.50.11    v3         fa2/1`
	`2     172.20.40.20    v2         Router`
	`switch(config)#`
	Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 50.
		
		Example
		• This command displays the querier IP address, version, and port servicing each VLAN.
		`switch>show ip igmp snooping querier`
		`Vlan  IP Address       Version  Port`
		`----------------------------------------`
		`1     172.17.0.37      v2       Po1`
		`20    172.17.20.1      v2       Po1`
		`26    172.17.26.1      v2       Cpu`
		`2028  172.17.255.29    v2       Po1`
		`switch>`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1860.

<table>
<tr>
<th>Copyright Registration Information</th>
<th>Cisco</th>
<th>Arista</th>
</tr>
<tr>
<td>

Cisco NX-OS 6.2

Effective date of registration: 11/13/2014

</td>
<td>



aaa group server tacacs+

To create a TACACS+ server group and enter TACACS+ server group configuration mode, use the **aaa group server tacacs+** command. To delete a TACACS+ server group, use the **no** form of this command.

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Syntax Description

group-name	TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.

Defaults

None

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

This command does not require a license.

Examples

This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:

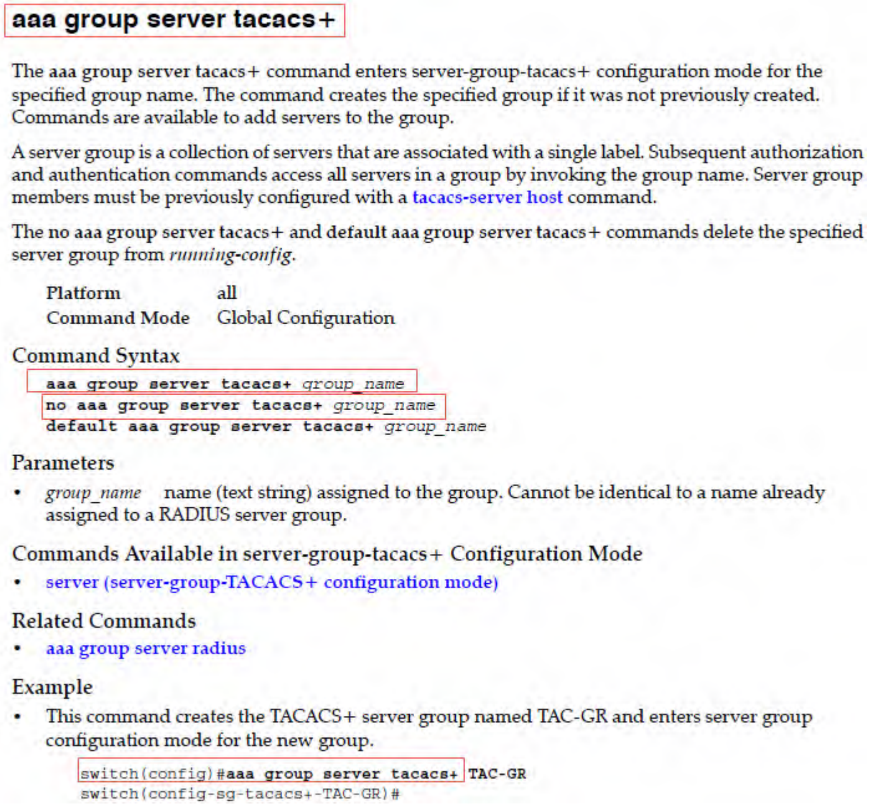
```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-radius)#
```

This example shows how to delete a TACACS+ server group:

```
switch# configure terminal
switch(config)# no aaa group server tacacs+ TacServer
```

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-34.

</td>
<td>



aaa group server tacacs+

The aaa group server tacacs+ command enters server-group-tacacs+ configuration mode for the specified group name. The command creates the specified group if it was not previously created. Commands are available to add servers to the group.

A server group is a collection of servers that are associated with a single label. Subsequent authorization and authentication commands access all servers in a group by invoking the group name. Server group members must be previously configured with a tacacs-server host command.

The no aaa group server tacacs+ and default aaa group server tacacs+ commands delete the specified server group from *running-config*.

Platform	all
Command Mode	Global Configuration

Command Syntax

```
aaa group server tacacs+ group_name
no aaa group server tacacs+ group_name
default aaa group server tacacs+ group_name
```

Parameters

- *group_name* name (text string) assigned to the group. Cannot be identical to a name already assigned to a RADIUS server group.

Commands Available in server-group-tacacs+ Configuration Mode

- server (server-group-TACACS+ configuration mode)

Related Commands

- aaa group server radius

Example

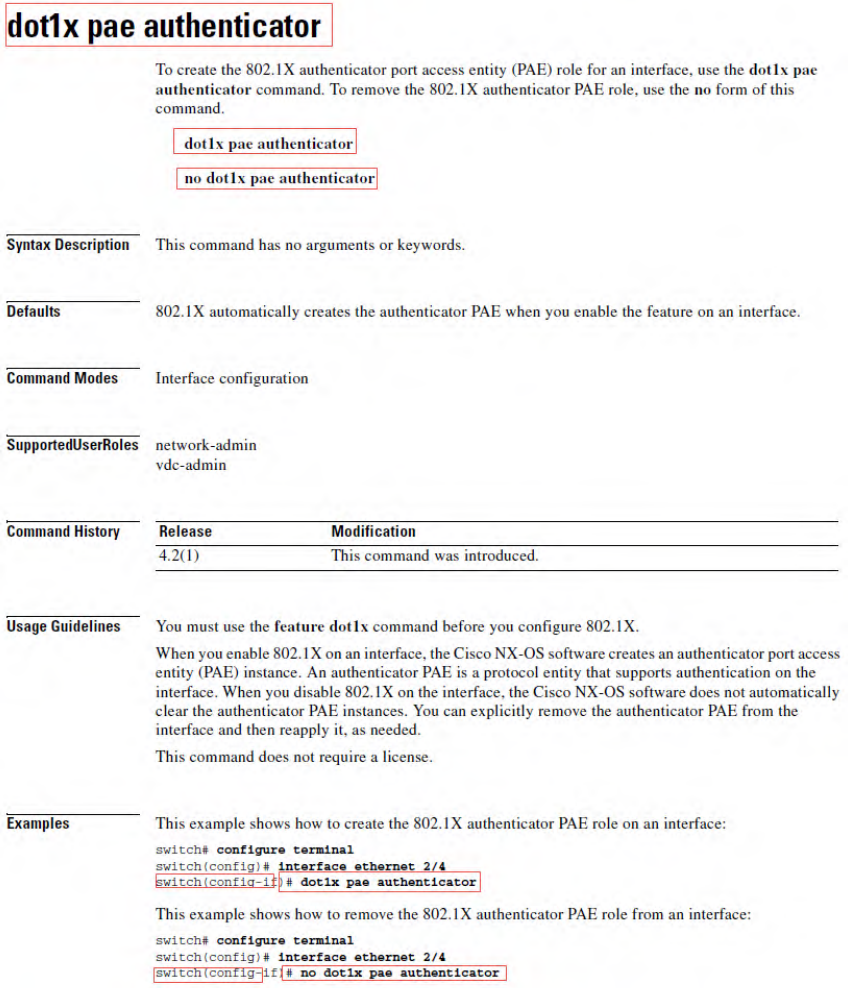
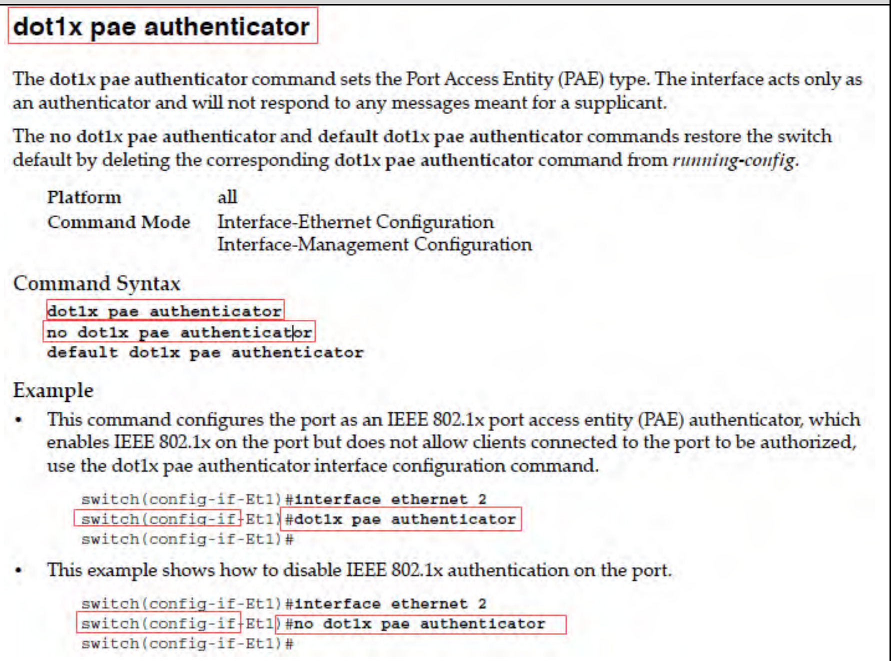
- This command creates the TACACS+ server group named TAC-GR and enters server group configuration mode for the new group.

```
switch(config)#aaa group server tacacs+ TAC-GR
switch(config-sg-tacacs+-TAC-GR)#
```

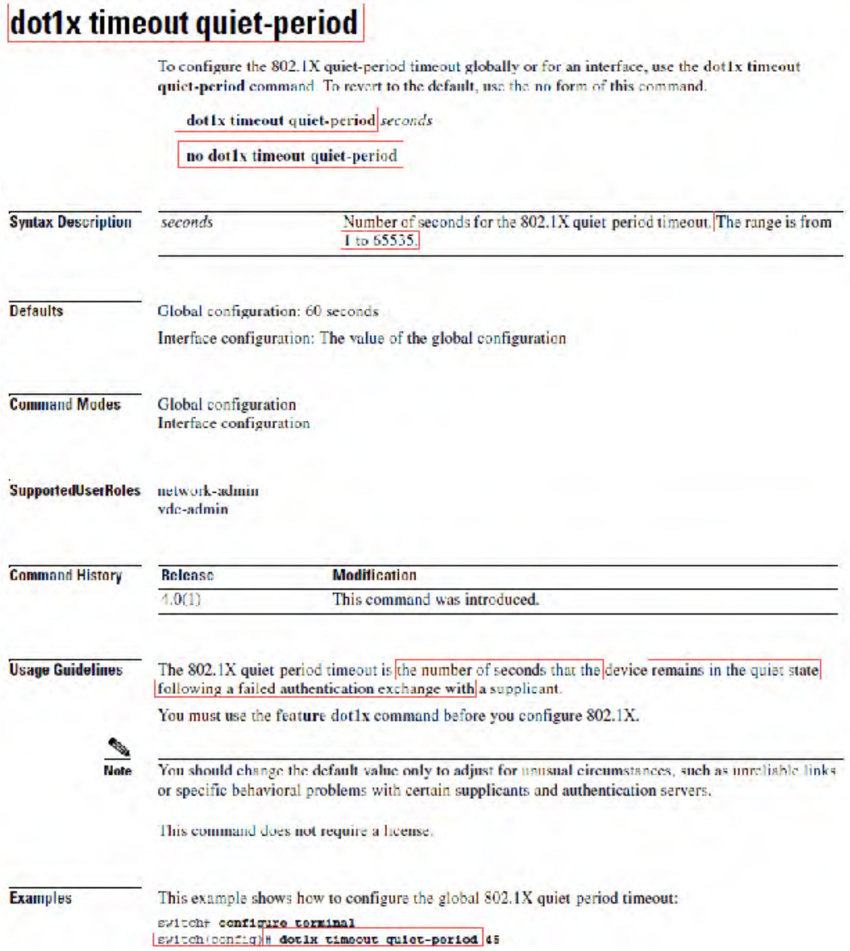
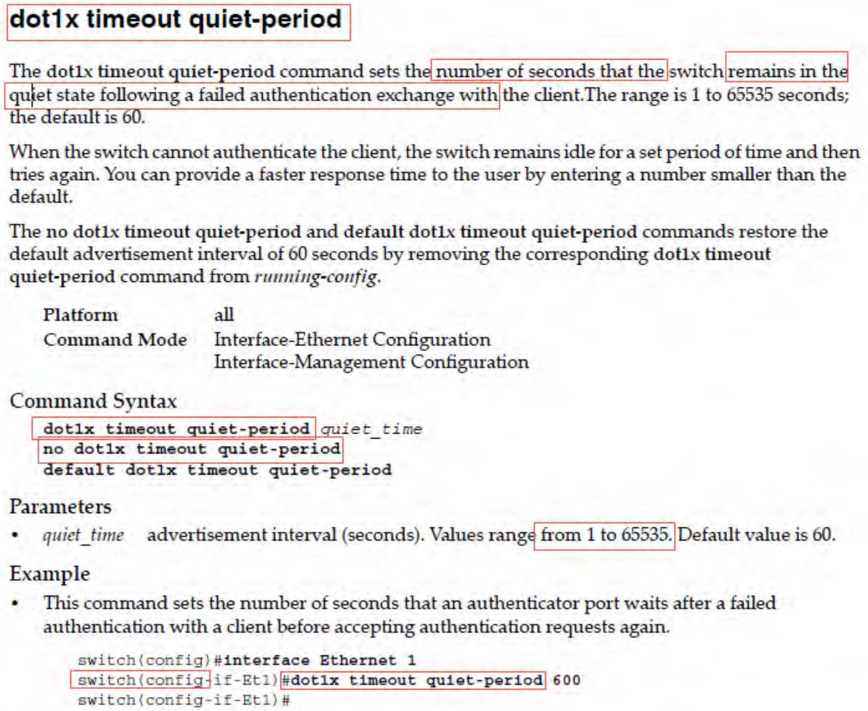
Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 225.

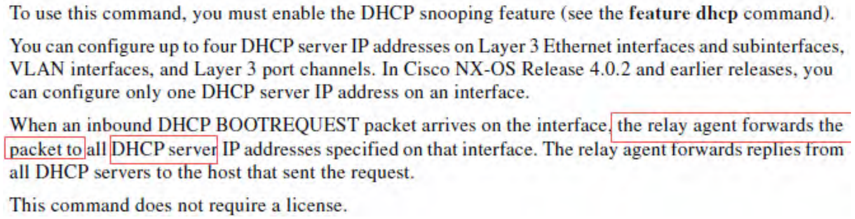
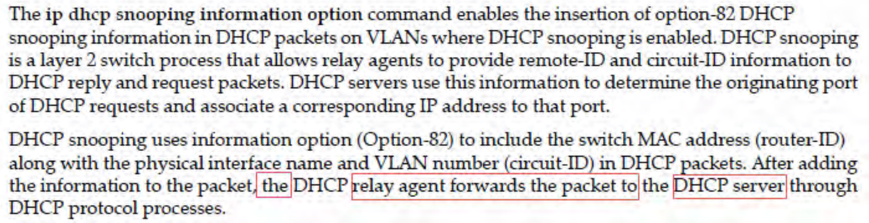
</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista

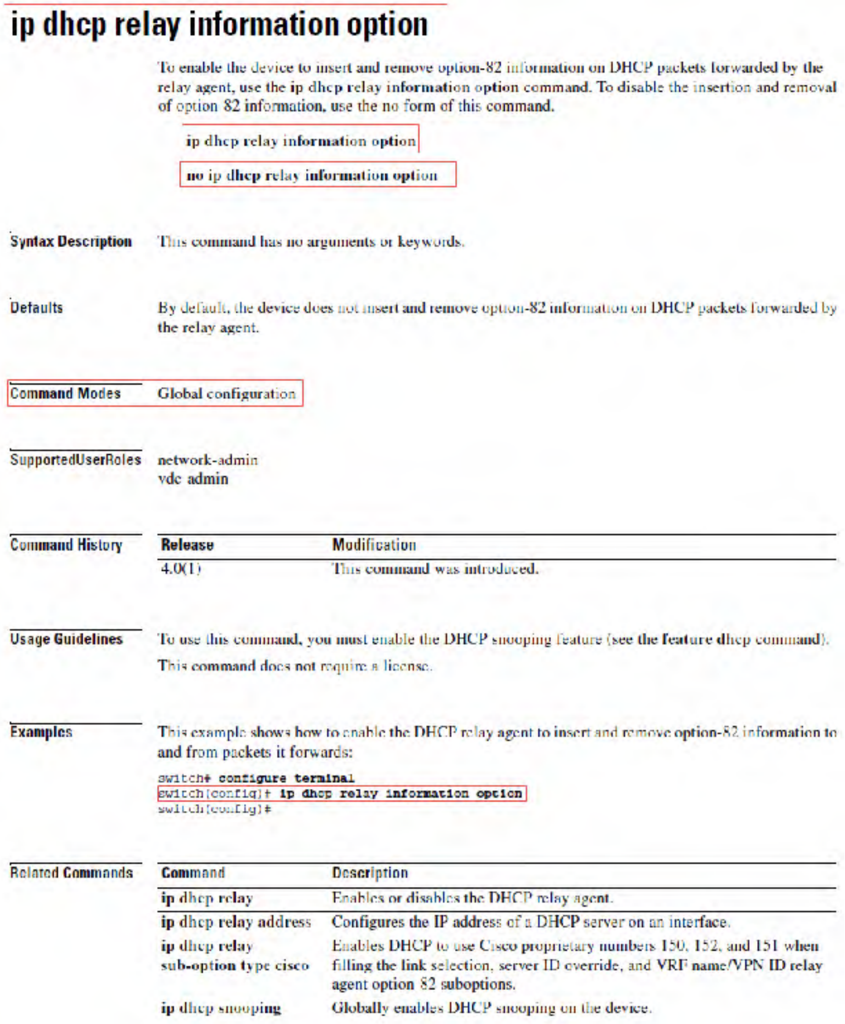
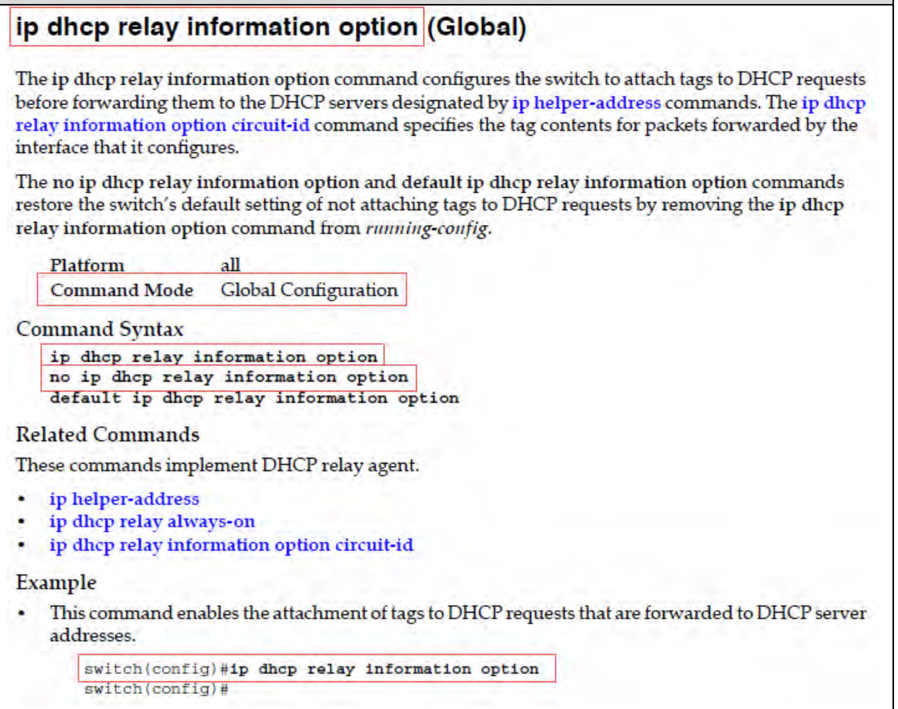
Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	dot1x pae authenticator
	To create the 802.1X authenticator port access entity (PAE) role for an interface, use the **dot1x pae authenticator** command. To remove the 802.1X authenticator PAE role, use the **no** form of this command.
	dot1x pae authenticator
	no dot1x pae authenticator
	Syntax Description This command has no arguments or keywords.
	Defaults 802.1X automatically creates the authenticator PAE when you enable the feature on an interface.
	Command Modes Interface configuration
	SupportedUserRoles network-admin
	vdc-admin
	Command History **Release** / **Modification**
	4.2(1) / This command was introduced.
	Usage Guidelines You must use the **feature dot1x** command before you configure 802.1X.
	When you enable 802.1X on an interface, the Cisco NX-OS software creates an authenticator port access entity (PAE) instance. An authenticator PAE is a protocol entity that supports authentication on the interface. When you disable 802.1X on the interface, the Cisco NX-OS software does not automatically clear the authenticator PAE instances. You can explicitly remove the authenticator PAE from the interface and then reapply it, as needed.
	This command does not require a license.
	Examples This example shows how to create the 802.1X authenticator PAE role on an interface:
	`switch# configure terminal`
	`switch(config)# interface ethernet 2/4`
	`switch(config-if)# dot1x pae authenticator`
	This example shows how to remove the 802.1X authenticator PAE role from an interface:
	`switch# configure terminal`
	`switch(config)# interface ethernet 2/4`
	`switch(config-if)# no dot1x pae authenticator`
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-191.
		
		dot1x pae authenticator
		The **dot1x pae authenticator** command sets the Port Access Entity (PAE) type. The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.
		The **no dot1x pae authenticator** and **default dot1x pae authenticator** commands restore the switch default by deleting the corresponding **dot1x pae authenticator** command from *running-config*.
		Platform all
		Command Mode Interface-Ethernet Configuration
		Interface-Management Configuration
		Command Syntax
		`dot1x pae authenticator`
		`no dot1x pae authenticator`
		`default dot1x pae authenticator`
		Example
		• This command configures the port as an IEEE 802.1x port access entity (PAE) authenticator, which enables IEEE 802.1x on the port but does not allow clients connected to the port to be authorized, use the dot1x pae authenticator interface configuration command.
		`switch(config-if-Et1)#interface ethernet 2`
		`switch(config-if-Et1)#dot1x pae authenticator`
		`switch(config-if-Et1)#`
		• This example shows how to disable IEEE 802.1x authentication on the port.
		`switch(config-if-Et1)#interface ethernet 2`
		`switch(config-if-Et1)#no dot1x pae authenticator`
		`switch(config-if-Et1)#`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 566.

Copyright Registration Information	Cisco	Arista

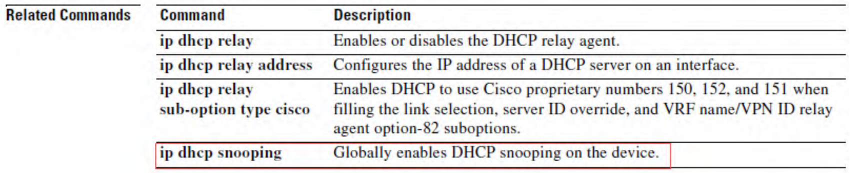
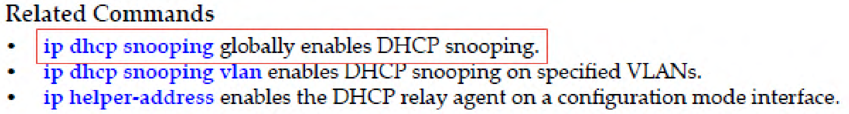
Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	dot1x timeout quiet-period
	To configure the 802.1X quiet-period timeout globally or for an interface, use the **dot1x timeout quiet-period** command. To revert to the default, use the **no** form of this command.
	dot1x timeout quiet-period *seconds*
	no dot1x timeout quiet-period
	Syntax Description *seconds* Number of seconds for the 802.1X quiet period timeout. The range is from 1 to 65535.
	Defaults Global configuration: 60 seconds
	Interface configuration: The value of the global configuration
	Command Modes Global configuration
	Interface configuration
	SupportedUserRoles network-admin
	vdc-admin
	Command History **Release** **Modification**
	4.0(1) This command was introduced.
	Usage Guidelines The 802.1X quiet period timeout is the number of seconds that the device remains in the quiet state following a failed authentication exchange with a supplicant.
	You must use the **feature dot1x** command before you configure 802.1X.
	Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.
	This command does not require a license.
	Examples This example shows how to configure the global 802.1X quiet period timeout:
	`switch# configure terminal`
	`switch(config)# dotlx timeout quiet-period 45`
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-200.
		
		dot1x timeout quiet-period
		The **dot1x timeout quiet-period** command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.The range is 1 to 65535 seconds; the default is 60.
		When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default.
		The **no dot1x timeout quiet-period** and **default dot1x timeout quiet-period** commands restore the default advertisement interval of 60 seconds by removing the corresponding **dot1x timeout quiet-period** command from ***running-config***.
		Platform all
		Command Mode Interface-Ethernet Configuration
		Interface-Management Configuration
		Command Syntax
		`dot1x timeout quiet-period quiet_time`
		`no dot1x timeout quiet-period`
		`default dot1x timeout quiet-period`
		Parameters
		• *quiet_time* advertisement interval (seconds). Values range from 1 to 65535. Default value is 60.
		Example
		• This command sets the number of seconds that an authenticator port waits after a failed authentication with a client before accepting authentication requests again.
		`switch(config)#interface Ethernet 1`
		`switch(config-if-Et1)#dot1x timeout quiet-period 600`
		`switch(config-if-Et1)#`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 569.

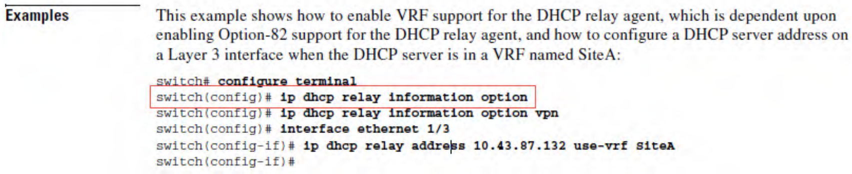
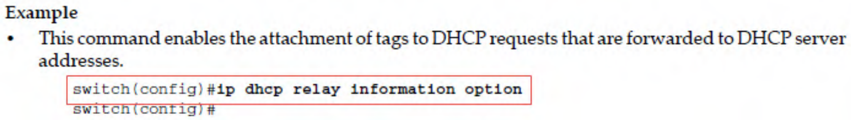
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 To use this command, you must enable the DHCP snooping feature (see the **feature dhcp** command). You can configure up to four DHCP server IP addresses on Layer 3 Ethernet interfaces and subinterfaces, VLAN interfaces, and Layer 3 port channels. In Cisco NX-OS Release 4.0.2 and earlier releases, you can configure only one DHCP server IP address on an interface. When an inbound DHCP BOOTREQUEST packet arrives on the interface, the relay agent forwards the packet to all DHCP server IP addresses specified on that interface. The relay agent forwards replies from all DHCP servers to the host that sent the request. This command does not require a license. Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-309.	 The **ip dhcp snooping information option** command enables the insertion of option-82 DHCP snooping information in DHCP packets on VLANs where DHCP snooping is enabled. DHCP snooping is a layer 2 switch process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP snooping uses information option (Option-82) to include the switch MAC address (router-ID) along with the physical interface name and VLAN number (circuit-ID) in DHCP packets. After adding the information to the packet, the DHCP relay agent forwards the packet to the DHCP server through DHCP protocol processes. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1270.

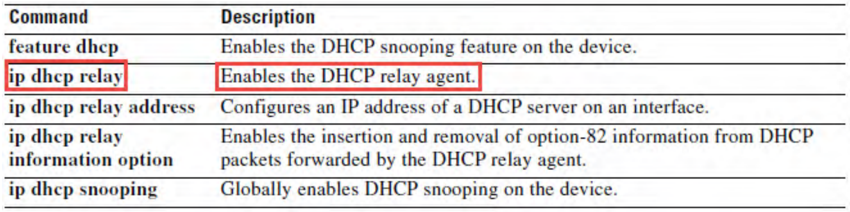
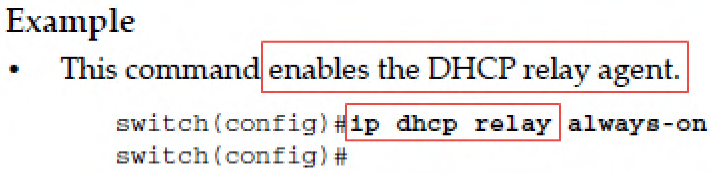
Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	ip dhcp relay information option
	To enable the device to insert and remove option-82 information on DHCP packets forwarded by the relay agent, use the **ip dhcp relay information option** command. To disable the insertion and removal of option 82 information, use the **no** form of this command.
	ip dhcp relay information option
	no ip dhcp relay information option
	Syntax Description This command has no arguments or keywords.
	Defaults By default, the device does not insert and remove option-82 information on DHCP packets forwarded by the relay agent.
	Command Modes Global configuration
	SupportedUserRoles network-admin
	vdc admin
	Command History **Release** **Modification**
	4.0(1) This command was introduced.
	Usage Guidelines To use this command, you must enable the DHCP snooping feature (see the **feature dhcp** command).
	This command does not require a license.
	Examples This example shows how to enable the DHCP relay agent to insert and remove option-82 information to and from packets it forwards:
	`switch# configure terminal`
	`switch(config)# ip dhcp relay information option`
	`switch(config)#`
	Related Commands **Command** **Description**
	ip dhcp relay Enables or disables the DHCP relay agent.
	ip dhcp relay address Configures the IP address of a DHCP server on an interface.
	ip dhcp relay sub-option type cisco Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option 82 suboptions.
	ip dhcp snooping Globally enables DHCP snooping on the device.
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-311.
		
		ip dhcp relay information option (Global)
		The **ip dhcp relay information option** command configures the switch to attach tags to DHCP requests before forwarding them to the DHCP servers designated by **ip helper-address** commands. The **ip dhcp relay information option circuit-id** command specifies the tag contents for packets forwarded by the interface that it configures.
		The **no ip dhcp relay information option** and **default ip dhcp relay information option** commands restore the switch's default setting of not attaching tags to DHCP requests by removing the **ip dhcp relay information option** command from *running-config*.
		Platform all
		Command Mode Global Configuration
		Command Syntax
		`ip dhcp relay information option`
		`no ip dhcp relay information option`
		`default ip dhcp relay information option`
		Related Commands
		These commands implement DHCP relay agent.
		• **ip helper-address**
		• **ip dhcp relay always-on**
		• **ip dhcp relay information option circuit-id**
		Example
		• This command enables the attachment of tags to DHCP requests that are forwarded to DHCP server addresses.
		`switch(config)#ip dhcp relay information option`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1264.

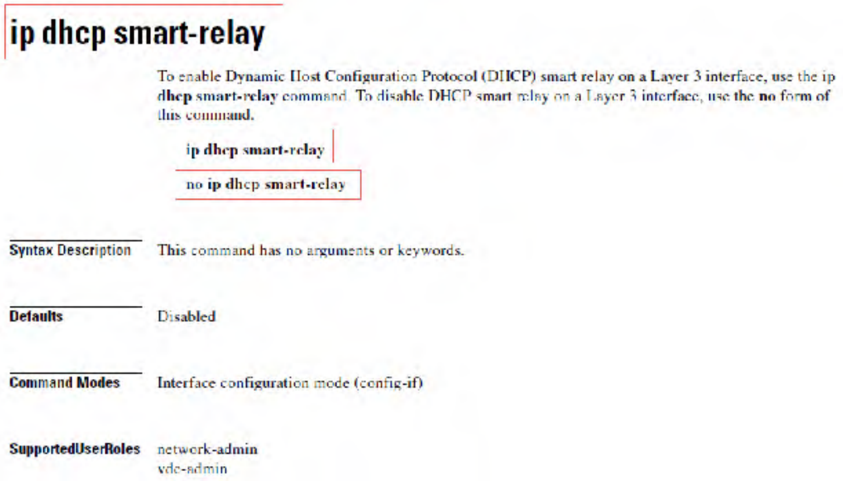
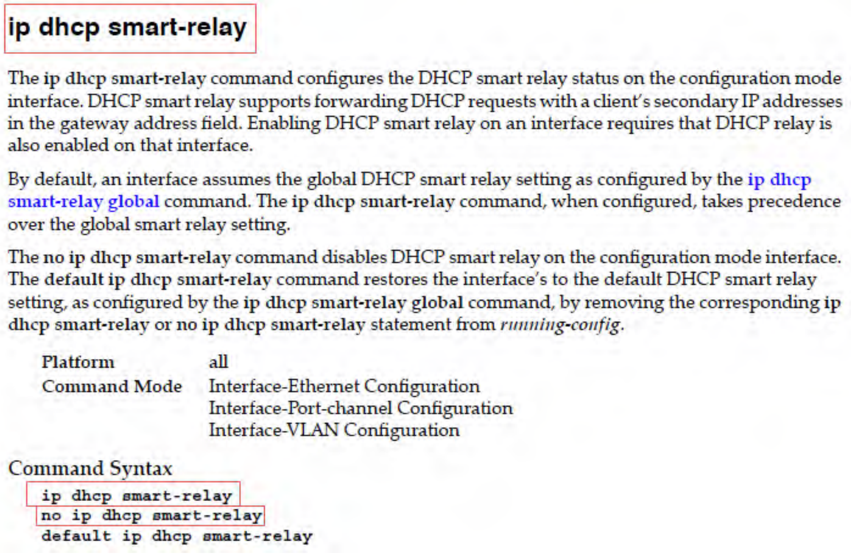
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 6.2

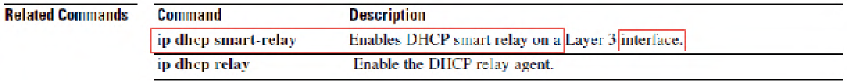
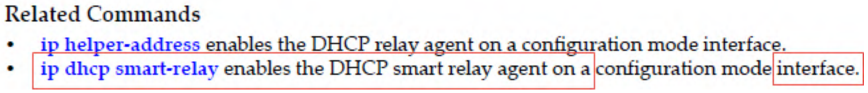
Effective date of registration: 11/13/2014</td>
<td>

<b>Related Commands</b>
<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>ip dhcp relay</td><td>Enables or disables the DHCP relay agent.</td></tr>
<tr><td>ip dhcp relay address</td><td>Configures the IP address of a DHCP server on an interface.</td></tr>
<tr><td>ip dhcp relay sub-option type cisco</td><td>Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.</td></tr>
<tr><td>ip dhcp snooping</td><td>Globally enables DHCP snooping on the device.</td></tr>
</table>
Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-311.
</td>
<td>

Related Commands
<ul>
<li>ip dhcp snooping globally enables DHCP snooping.</li>
<li>ip dhcp snooping vlan enables DHCP snooping on specified VLANs.</li>
<li>ip helper-address enables the DHCP relay agent on a configuration mode interface.</li>
</ul>
Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1270.
</td>
</tr>
<tr>
<td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td>
<td>

<b>Examples</b>
This example shows how to enable VRF support for the DHCP relay agent, which is dependent upon enabling Option-82 support for the DHCP relay agent, and how to configure a DHCP server address on a Layer 3 interface when the DHCP server is in a VRF named SiteA:
<pre>
switch# configure terminal
switch(config)# ip dhcp relay information option
switch(config)# ip dhcp relay information option vpn
switch(config)# interface ethernet 1/3
switch(config-if)# ip dhcp relay address 10.43.87.132 use-vrf SiteA
switch(config-if)#
</pre>
Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-314.
</td>
<td>

Example
<ul>
<li>This command enables the attachment of tags to DHCP requests that are forwarded to DHCP server addresses.</li>
</ul>
<pre>
switch(config)#ip dhcp relay information option
switch(config)#
</pre>
Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1237.
</td>
</tr>
<tr>
<td>Cisco NX-OS 6.2

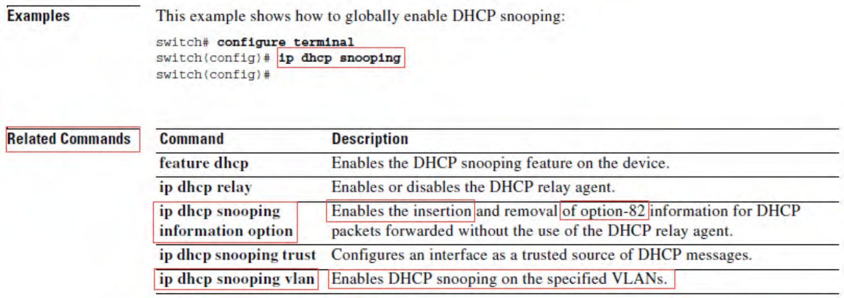
Effective date of registration: 11/13/2014</td>
<td>

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>feature dhcp</td><td>Enables the DHCP snooping feature on the device.</td></tr>
<tr><td>ip dhcp relay</td><td>Enables the DHCP relay agent.</td></tr>
<tr><td>ip dhcp relay address</td><td>Configures an IP address of a DHCP server on an interface.</td></tr>
<tr><td>ip dhcp relay information option</td><td>Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.</td></tr>
<tr><td>ip dhcp snooping</td><td>Globally enables DHCP snooping on the device.</td></tr>
</table>
Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-317.
</td>
<td>

Example
<ul>
<li>This command enables the DHCP relay agent.</li>
</ul>
<pre>
switch(config)#ip dhcp relay always-on
switch(config)#
</pre>
Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1263.
</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista

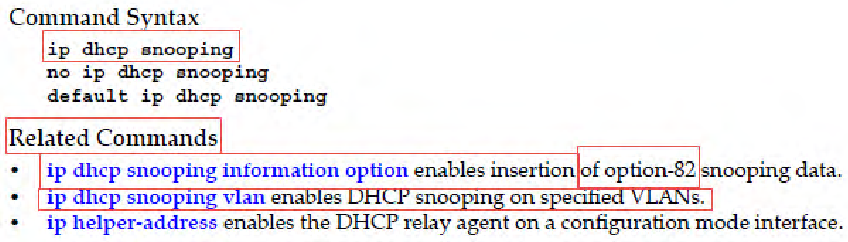
Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	ip dhcp smart-relay
	To enable Dynamic Host Configuration Protocol (DHCP) smart relay on a Layer 3 interface, use the **ip dhcp smart-relay** command. To disable DHCP smart relay on a Layer 3 interface, use the **no** form of this command.
	ip dhcp smart-relay
	no ip dhcp smart-relay
	Syntax Description This command has no arguments or keywords.
	Defaults Disabled
	Command Modes Interface configuration mode (config-if)
	SupportedUserRoles network-admin
	vdc-admin
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-319.
		
		ip dhcp smart-relay
		The **ip dhcp smart-relay** command configures the DHCP smart relay status on the configuration mode interface. DHCP smart relay supports forwarding DHCP requests with a client's secondary IP addresses in the gateway address field. Enabling DHCP smart relay on an interface requires that DHCP relay is also enabled on that interface.
		By default, an interface assumes the global DHCP smart relay setting as configured by the ip dhcp smart-relay global command. The **ip dhcp smart-relay** command, when configured, takes precedence over the global smart relay setting.
		The **no ip dhcp smart-relay** command disables DHCP smart relay on the configuration mode interface. The **default ip dhcp smart-relay** command restores the interface's to the default DHCP smart relay setting, as configured by the **ip dhcp smart-relay global** command, by removing the corresponding **ip dhcp smart-relay** or **no ip dhcp smart-relay** statement from *running-config*.
		Platform all
		Command Mode Interface-Ethernet Configuration
		Interface-Port-channel Configuration
		Interface-VLAN Configuration
		Command Syntax
		`ip dhcp smart-relay`
		`no ip dhcp smart-relay`
		`default ip dhcp smart-relay`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1266.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Related Commands** **Command** — **Description** ip dhcp smart-relay — Enables DHCP smart relay on a Layer 3 interface. ip dhcp relay — Enable the DHCP relay agent. Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-322.	 Related Commands • ip helper-address enables the DHCP relay agent on a configuration mode interface. • ip dhcp smart-relay enables the DHCP smart relay agent on a configuration mode interface. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1268.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td>
<td>
<b>Examples</b> This example shows how to globally enable DHCP snooping:
<code>switch# <b>configure terminal</b></code>
<code>switch(config)# <b>ip dhcp snooping</b></code>
<code>switch(config)#</code>

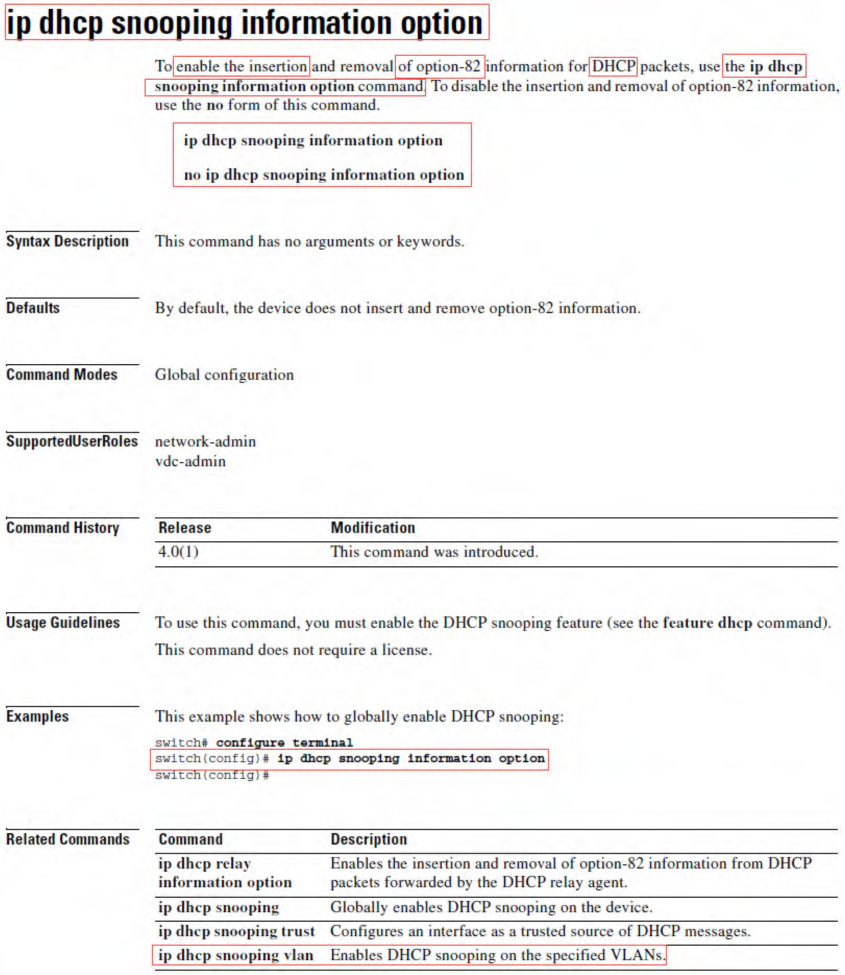
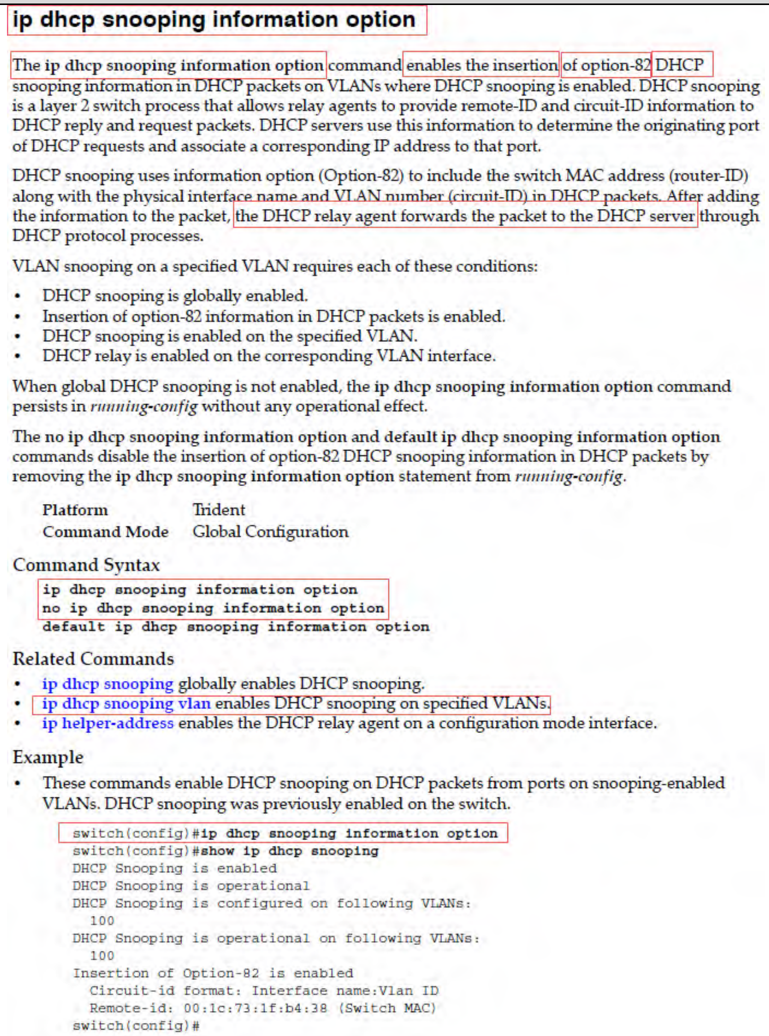
<b>Related Commands</b>
<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>feature dhcp</b></td><td>Enables the DHCP snooping feature on the device.</td></tr>
<tr><td><b>ip dhcp relay</b></td><td>Enables or disables the DHCP relay agent.</td></tr>
<tr><td><b>ip dhcp snooping information option</b></td><td>Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.</td></tr>
<tr><td><b>ip dhcp snooping trust</b></td><td>Configures an interface as a trusted source of DHCP messages.</td></tr>
<tr><td><b>ip dhcp snooping vlan</b></td><td>Enables DHCP snooping on the specified VLANs.</td></tr>
</table>

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-323.</td>
<td>
Command Syntax
<code>ip dhcp snooping</code>
<code>no ip dhcp snooping</code>
<code>default ip dhcp snooping</code>

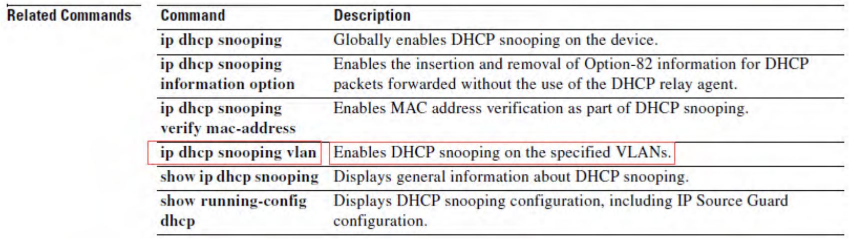
Related Commands
• ip dhcp snooping information option enables insertion of option-82 snooping data.
• ip dhcp snooping vlan enables DHCP snooping on specified VLANs.
• ip helper-address enables the DHCP relay agent on a configuration mode interface.

Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1269.</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista

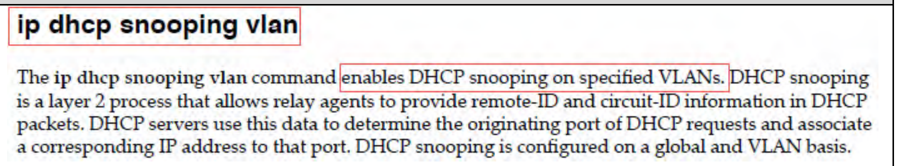
Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	ip dhcp snooping information option
	To enable the insertion and removal of option-82 information for DHCP packets, use the **ip dhcp snooping information option** command. To disable the insertion and removal of option-82 information, use the **no** form of this command.
	ip dhcp snooping information option
	no ip dhcp snooping information option
	Syntax Description This command has no arguments or keywords.
	Defaults By default, the device does not insert and remove option-82 information.
	Command Modes Global configuration
	SupportedUserRoles network-admin
	vdc-admin
	Command History **Release** **Modification**
	4.0(1) This command was introduced.
	Usage Guidelines To use this command, you must enable the DHCP snooping feature (see the **feature dhcp** command).
	This command does not require a license.
	Examples This example shows how to globally enable DHCP snooping:
	`switch# configure terminal`
	`switch(config)# ip dhcp snooping information option`
	`switch(config)#`
	Related Commands **Command** **Description**
	ip dhcp relay information option Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.
	ip dhcp snooping Globally enables DHCP snooping on the device.
	ip dhcp snooping trust Configures an interface as a trusted source of DHCP messages.
	ip dhcp snooping vlan Enables DHCP snooping on the specified VLANs.
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-325.
		
		ip dhcp snooping information option
		The **ip dhcp snooping information option** command enables the insertion of option-82 DHCP snooping information in DHCP packets on VLANs where DHCP snooping is enabled. DHCP snooping is a layer 2 switch process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port.
		DHCP snooping uses information option (Option-82) to include the switch MAC address (router-ID) along with the physical interface name and VLAN number (circuit-ID) in DHCP packets. After adding the information to the packet, the DHCP relay agent forwards the packet to the DHCP server through DHCP protocol processes.
		VLAN snooping on a specified VLAN requires each of these conditions:
		• DHCP snooping is globally enabled.
		• Insertion of option-82 information in DHCP packets is enabled.
		• DHCP snooping is enabled on the specified VLAN.
		• DHCP relay is enabled on the corresponding VLAN interface.
		When global DHCP snooping is not enabled, the **ip dhcp snooping information option** command persists in *running-config* without any operational effect.
		The **no ip dhcp snooping information option** and **default ip dhcp snooping information option** commands disable the insertion of option-82 DHCP snooping information in DHCP packets by removing the **ip dhcp snooping information option** statement from *running-config*.
		Platform Trident
		Command Mode Global Configuration
		Command Syntax
		`ip dhcp snooping information option`
		`no ip dhcp snooping information option`
		`default ip dhcp snooping information option`
		Related Commands
		• ip dhcp snooping globally enables DHCP snooping.
		• ip dhcp snooping vlan enables DHCP snooping on specified VLANs.
		• ip helper-address enables the DHCP relay agent on a configuration mode interface.
		Example
		• These commands enable DHCP snooping on DHCP packets from ports on snooping-enabled VLANs. DHCP snooping was previously enabled on the switch.
		`switch(config)#ip dhcp snooping information option`
		`switch(config)#show ip dhcp snooping`
		`DHCP Snooping is enabled`
		`DHCP Snooping is operational`
		`DHCP Snooping is configured on following VLANs:`
		`  100`
		`DHCP Snooping is operational on following VLANs:`
		`  100`
		`Insertion of Option-82 is enabled`
		`  Circuit-id format: Interface name:Vlan ID`
		`  Remote-id: 00:1c:73:1f:b4:38 (Switch MAC)`
		`switch(config)#`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1270.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td>
<td>


Related Commands

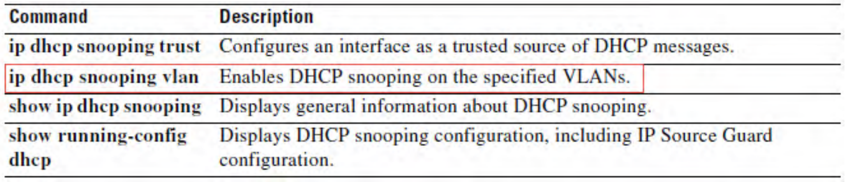
<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>ip dhcp snooping</td><td>Globally enables DHCP snooping on the device.</td></tr>
<tr><td>ip dhcp snooping information option</td><td>Enables the insertion and removal of Option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.</td></tr>
<tr><td>ip dhcp snooping verify mac-address</td><td>Enables MAC address verification as part of DHCP snooping.</td></tr>
<tr><td>ip dhcp snooping vlan</td><td>Enables DHCP snooping on the specified VLANs.</td></tr>
<tr><td>show ip dhcp snooping</td><td>Displays general information about DHCP snooping.</td></tr>
<tr><td>show running-config dhcp</td><td>Displays DHCP snooping configuration, including IP Source Guard configuration.</td></tr>
</table>

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-328.
</td>
<td>


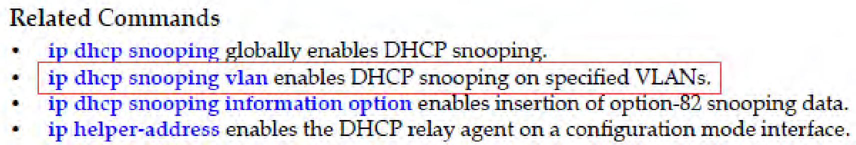
ip dhcp snooping vlan

The ip dhcp snooping vlan command enables DHCP snooping on specified VLANs. DHCP snooping is a layer 2 process that allows relay agents to provide remote-ID and circuit-ID information in DHCP packets. DHCP servers use this data to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP snooping is configured on a global and VLAN basis.

Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1271.
</td>
</tr>
<tr>
<td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td>
<td>


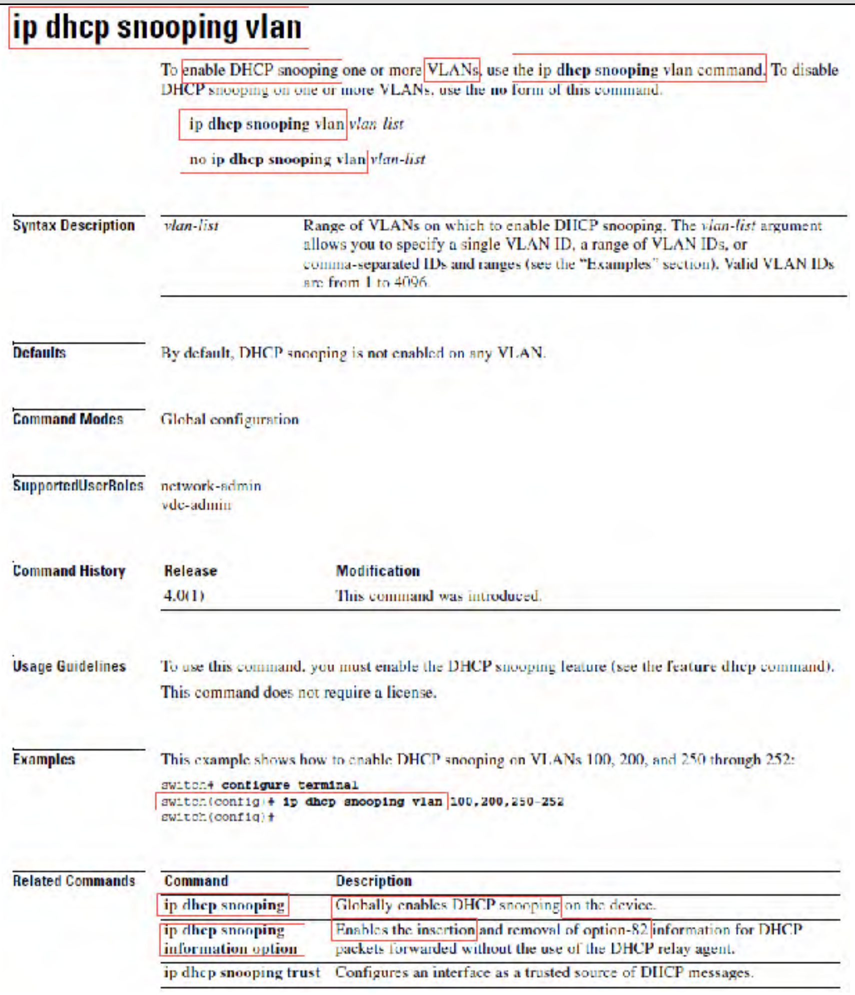
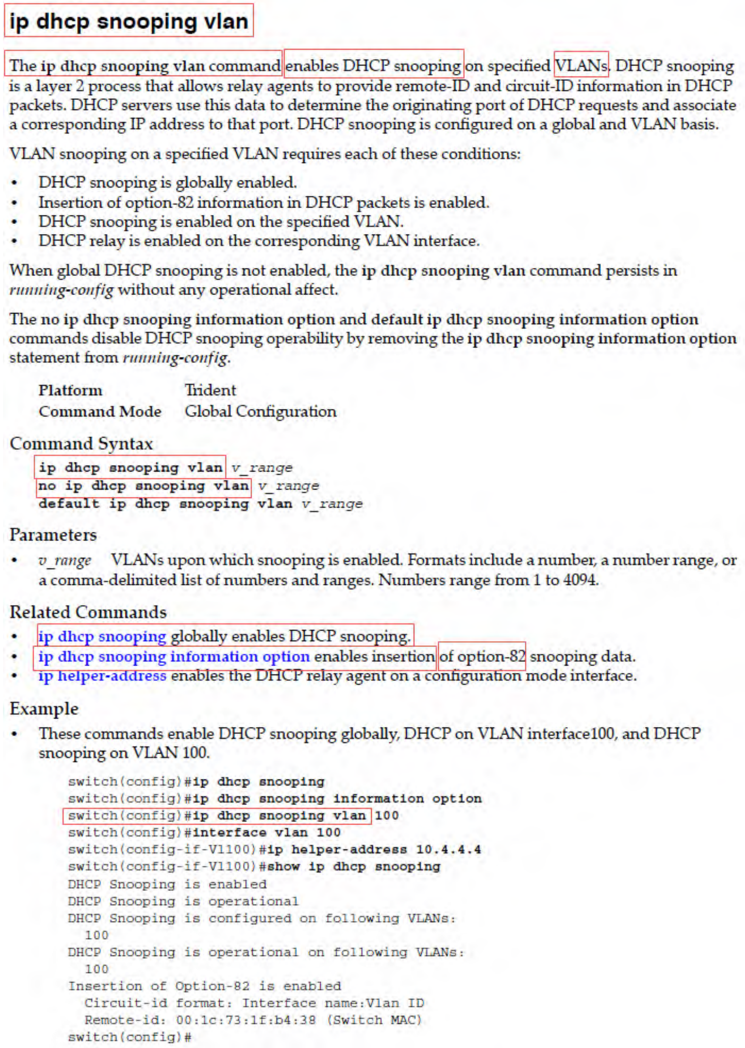
<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>ip dhcp snooping trust</td><td>Configures an interface as a trusted source of DHCP messages.</td></tr>
<tr><td>ip dhcp snooping vlan</td><td>Enables DHCP snooping on the specified VLANs.</td></tr>
<tr><td>show ip dhcp snooping</td><td>Displays general information about DHCP snooping.</td></tr>
<tr><td>show running-config dhcp</td><td>Displays DHCP snooping configuration, including IP Source Guard configuration.</td></tr>
</table>

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-330.
</td>
<td>


Related Commands

- ip dhcp snooping globally enables DHCP snooping.
- ip dhcp snooping vlan enables DHCP snooping on specified VLANs.
- ip dhcp snooping information option enables insertion of option-82 snooping data.
- ip helper-address enables the DHCP relay agent on a configuration mode interface.

Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1302.
</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-331.	 Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1302.

ip dhcp snooping vlan

To enable DHCP snooping one or more VLANs, use the ip **dhcp snooping** vlan command. To disable DHCP snooping on one or more VLANs, use the **no** form of this command.

ip **dhcp snooping** vlan *vlan list*

no ip **dhcp snooping** vlan *vlan-list*

Syntax Description

vlan-list	Range of VLANs on which to enable DHCP snooping. The *vlan-list* argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4096.

Defaults By default, DHCP snooping is not enabled on any VLAN.

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines To use this command, you must enable the DHCP snooping feature (see the **feature dhcp** command).

This command does not require a license.

Examples This example shows how to enable DHCP snooping on VLANs 100, 200, and 250 through 252:

```
switch# configure terminal
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping on the device.
ip dhcp snooping information option	Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.

ip dhcp snooping vlan

The ip dhcp snooping vlan command enables DHCP snooping on specified VLANs. DHCP snooping is a layer 2 process that allows relay agents to provide remote-ID and circuit-ID information in DHCP packets. DHCP servers use this data to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP snooping is configured on a global and VLAN basis.

VLAN snooping on a specified VLAN requires each of these conditions:

- DHCP snooping is globally enabled.
- Insertion of option-82 information in DHCP packets is enabled.
- DHCP snooping is enabled on the specified VLAN.
- DHCP relay is enabled on the corresponding VLAN interface.

When global DHCP snooping is not enabled, the ip dhcp snooping vlan command persists in *running-config* without any operational affect.

The no ip dhcp snooping information option and default ip dhcp snooping information option commands disable DHCP snooping operability by removing the ip dhcp snooping information option statement from *running-config*.

Platform	Trident
Command Mode	Global Configuration

Command Syntax

```
ip dhcp snooping vlan v_range
no ip dhcp snooping vlan v_range
default ip dhcp snooping vlan v_range
```

Parameters

- *v_range* VLANs upon which snooping is enabled. Formats include a number, a number range, or a comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.

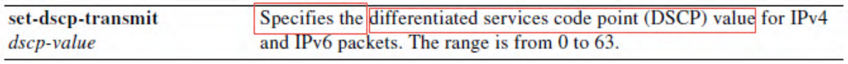
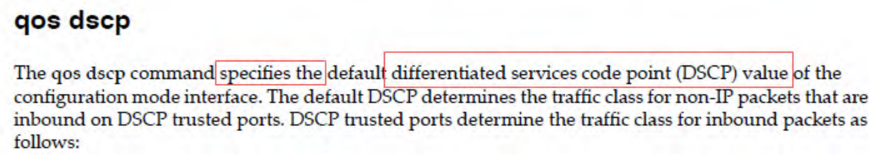
Related Commands

- ip dhcp snooping globally enables DHCP snooping.
- ip dhcp snooping information option enables insertion of option-82 snooping data.
- ip helper-address enables the DHCP relay agent on a configuration mode interface.

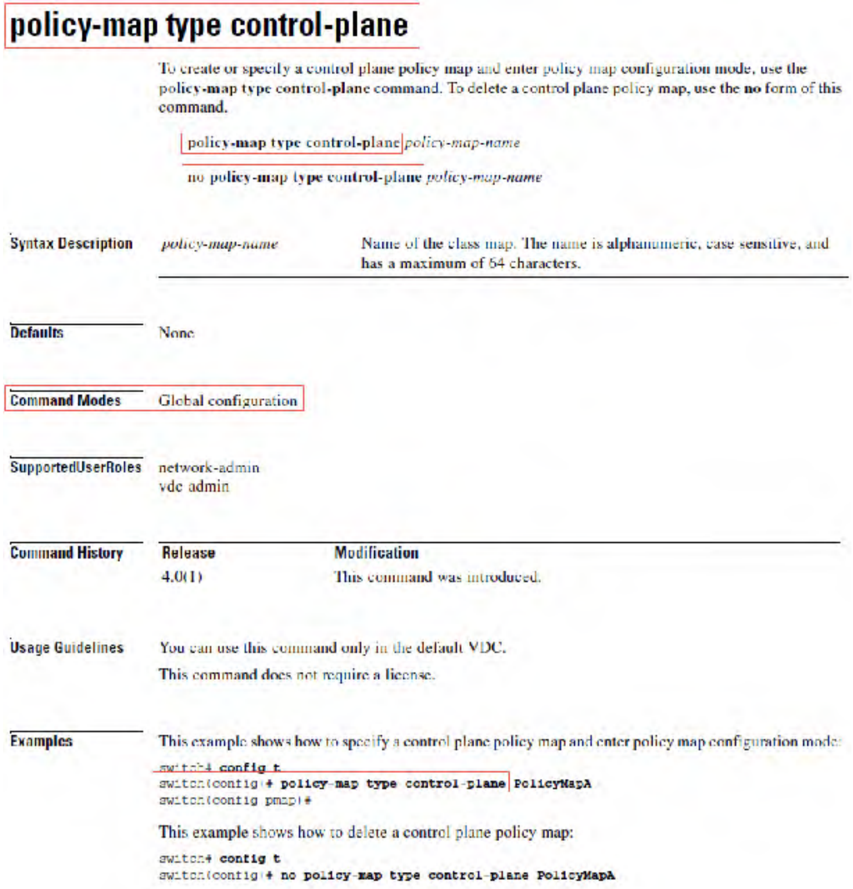
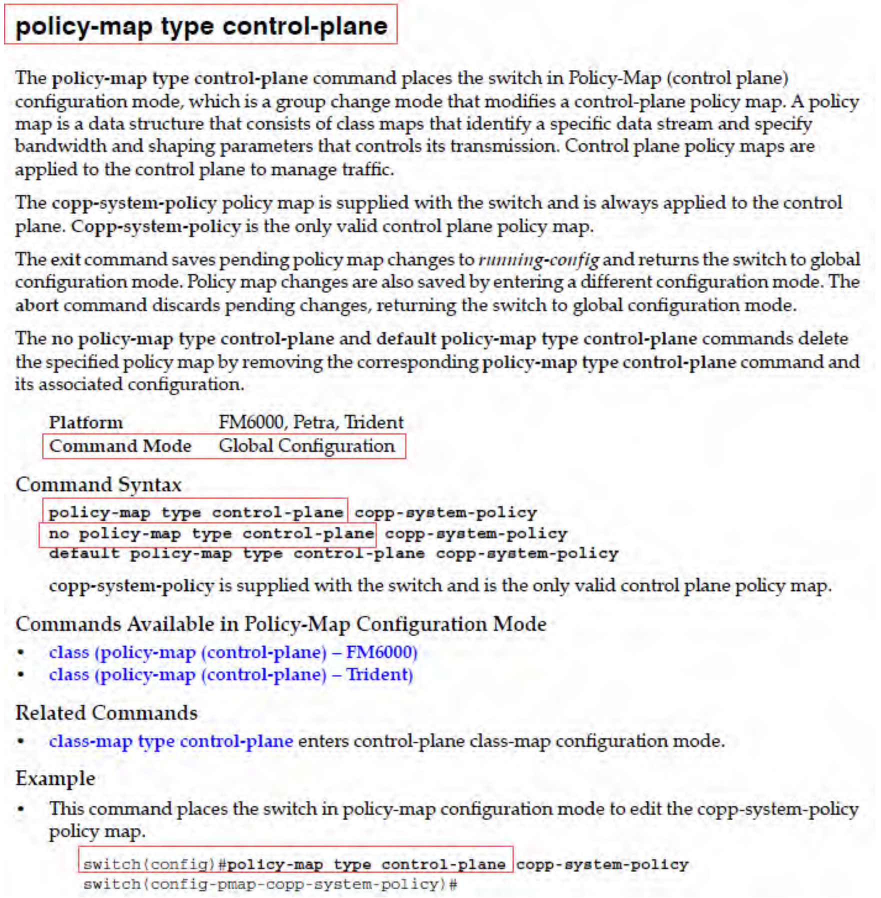
Example

- These commands enable DHCP snooping globally, DHCP on VLAN interface100, and DHCP snooping on VLAN 100.

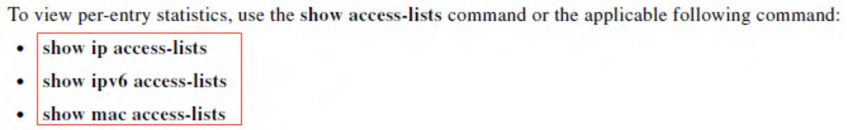
```
switch(config)#ip dhcp snooping
switch(config)#ip dhcp snooping information option
switch(config)#ip dhcp snooping vlan 100
switch(config)#interface vlan 100
switch(config-if-Vl100)#ip helper-address 10.4.4.4
switch(config-if-Vl100)#show ip dhcp snooping
DHCP Snooping is enabled
DHCP Snooping is operational
DHCP Snooping is configured on following VLANs:
  100
DHCP Snooping is operational on following VLANs:
  100
Insertion of Option-82 is enabled
  Circuit-id format: Interface name:Vlan ID
  Remote-id: 00:1c:73:1f:b4:38 (Switch MAC)
switch(config)#
```

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **set-dscp-transmit** *dscp-value* Specifies the differentiated services code point (DSCP) value for IPv4 and IPv6 packets. The range is from 0 to 63. Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-444.	 **qos dscp** The qos dscp command specifies the default differentiated services code point (DSCP) value of the configuration mode interface. The default DSCP determines the traffic class for non-IP packets that are inbound on DSCP trusted ports. DSCP trusted ports determine the traffic class for inbound packets as follows: Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1093.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	policy-map type control-plane
	To create or specify a control plane policy map and enter policy map configuration mode, use the **policy-map type control-plane** command. To delete a control plane policy map, use the **no** form of this command.
	policy-map type control-plane *policy-map-name*
	no policy-map type control-plane *policy-map-name*
	Syntax Description *policy-map-name* Name of the class map. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
	Defaults None
	Command Modes Global configuration
	SupportedUserRoles network-admin
	vdc admin
	Command History **Release** **Modification**
	4.0(1) This command was introduced.
	Usage Guidelines You can use this command only in the default VDC.
	This command does not require a license.
	Examples This example shows how to specify a control plane policy map and enter policy map configuration mode:
	`switch# config t`
	`switch(config)# policy-map type control-plane PolicyMapA`
	`switch(config pmap)#`
	This example shows how to delete a control plane policy map:
	`switch# config t`
	`switch(config)# no policy-map type control-plane PolicyMapA`
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-448.
		
		policy-map type control-plane
		The **policy-map type control-plane** command places the switch in Policy-Map (control plane) configuration mode, which is a group change mode that modifies a control-plane policy map. A policy map is a data structure that consists of class maps that identify a specific data stream and specify bandwidth and shaping parameters that controls its transmission. Control plane policy maps are applied to the control plane to manage traffic.
		The **copp-system-policy** policy map is supplied with the switch and is always applied to the control plane. Copp-system-policy is the only valid control plane policy map.
		The **exit** command saves pending policy map changes to *running-config* and returns the switch to global configuration mode. Policy map changes are also saved by entering a different configuration mode. The **abort** command discards pending changes, returning the switch to global configuration mode.
		The **no policy-map type control-plane** and **default policy-map type control-plane** commands delete the specified policy map by removing the corresponding **policy-map type control-plane** command and its associated configuration.
		Platform FM6000, Petra, Trident
		Command Mode Global Configuration
		Command Syntax
		`policy-map type control-plane copp-system-policy`
		`no policy-map type control-plane copp-system-policy`
		`default policy-map type control-plane copp-system-policy`
		copp-system-policy is supplied with the switch and is the only valid control plane policy map.
		Commands Available in Policy-Map Configuration Mode
		- class (policy-map (control-plane) – FM6000)
		- class (policy-map (control-plane) – Trident)
		Related Commands
		- class-map type control-plane enters control-plane class-map configuration mode.
		Example
		- This command places the switch in policy-map configuration mode to edit the copp-system-policy policy map.
		`switch(config)#policy-map type control-plane copp-system-policy`
		`switch(config-pmap-copp-system-policy)#`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1194.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 6.2
Effective date of registration: 11/13/2014</td>
<td>

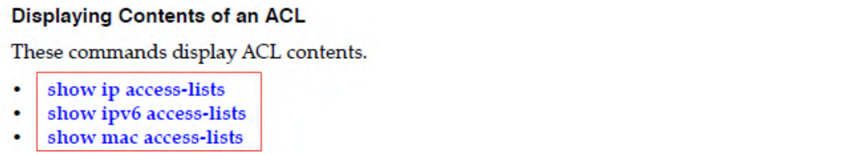


To view per-entry statistics, use the **show access-lists** command or the applicable following command:

- **show ip access-lists**
- **show ipv6 access-lists**
- **show mac access-lists**

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-517.

</td>
<td>



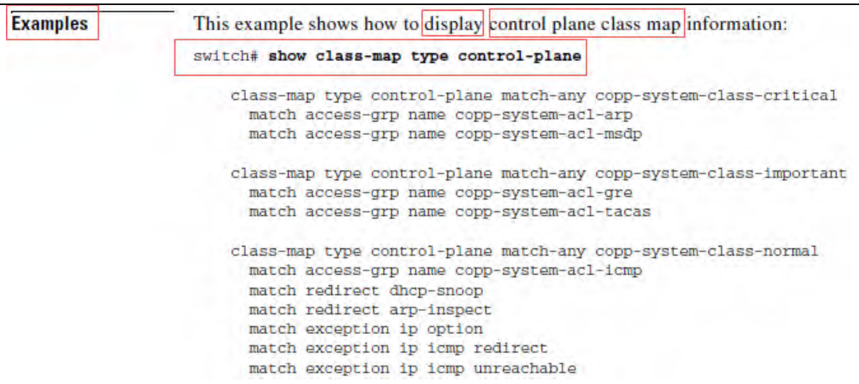
Displaying Contents of an ACL

These commands display ACL contents.

- **show ip access-lists**
- **show ipv6 access-lists**
- **show mac access-lists**

Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 845.

</td>
</tr>
<tr>
<td>Cisco NX-OS 6.2
Effective date of registration: 11/13/2014</td>
<td>



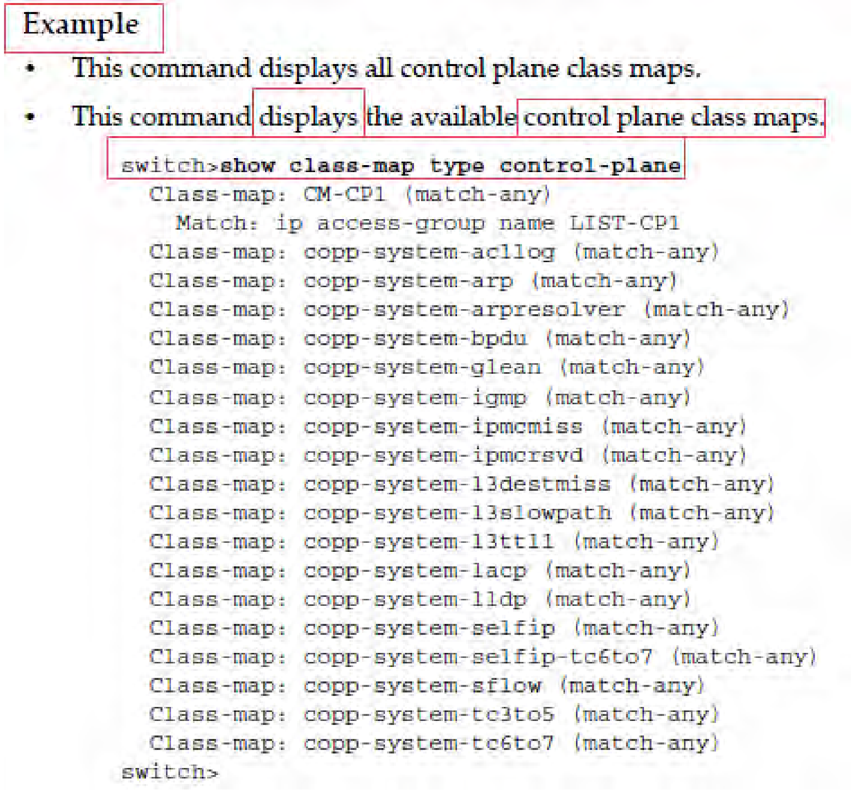
Examples

This example shows how to display control plane class map information:

```
switch# show class-map type control-plane

    class-map type control-plane match-any copp-system-class-critical
      match access-grp name copp-system-acl-arp
      match access-grp name copp-system-acl-msdp

    class-map type control-plane match-any copp-system-class-important
      match access-grp name copp-system-acl-gre
      match access-grp name copp-system-acl-tacas

    class-map type control-plane match-any copp-system-class-normal
      match access-grp name copp-system-acl-icmp
      match redirect dhcp-snoop
      match redirect arp-inspect
      match exception ip option
      match exception ip icmp redirect
      match exception ip icmp unreachable
```

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-552.

</td>
<td>



Example

- This command displays all control plane class maps.
- This command displays the available control plane class maps.

```
switch>show class-map type control-plane
  Class-map: CM-CP1 (match-any)
    Match: ip access-group name LIST-CP1
  Class-map: copp-system-acllog (match-any)
  Class-map: copp-system-arp (match-any)
  Class-map: copp-system-arpresolver (match-any)
  Class-map: copp-system-bpdu (match-any)
  Class-map: copp-system-glean (match-any)
  Class-map: copp-system-igmp (match-any)
  Class-map: copp-system-ipmcmiss (match-any)
  Class-map: copp-system-ipmcrsvd (match-any)
  Class-map: copp-system-l3destmiss (match-any)
  Class-map: copp-system-l3slowpath (match-any)
  Class-map: copp-system-l3ttl1 (match-any)
  Class-map: copp-system-lacp (match-any)
  Class-map: copp-system-lldp (match-any)
  Class-map: copp-system-selfip (match-any)
  Class-map: copp-system-selfip-tc6to7 (match-any)
  Class-map: copp-system-sflow (match-any)
  Class-map: copp-system-tc3to5 (match-any)
  Class-map: copp-system-tc6to7 (match-any)
switch>
```

Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1212.

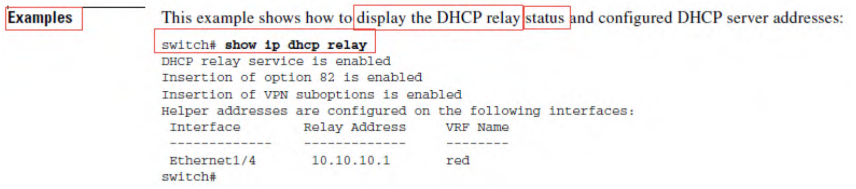
</td>
</tr>
</table>

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>

Cisco NX-OS 6.2

Effective date of registration: 11/13/2014

</td>
<td>

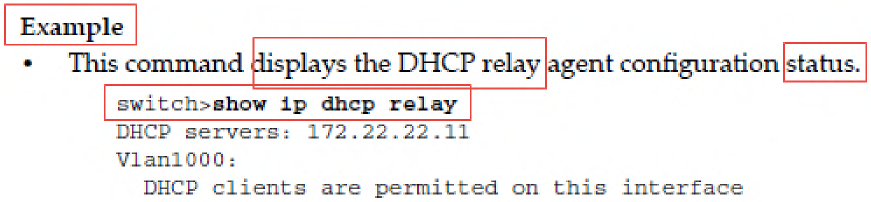


Examples This example shows how to display the DHCP relay status and configured DHCP server addresses:

```
switch# show ip dhcp relay
DHCP relay service is enabled
Insertion of option 82 is enabled
Insertion of VPN suboptions is enabled
Helper addresses are configured on the following interfaces:
 Interface         Relay Address      VRF Name
 -------------     -------------      --------
 Ethernet1/4        10.10.10.1        red
switch#
```

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-630.

</td>
<td>



Example

- This command displays the DHCP relay agent configuration status.

```
switch>show ip dhcp relay
DHCP servers: 172.22.22.11
Vlan1000:
  DHCP clients are permitted on this interface
```

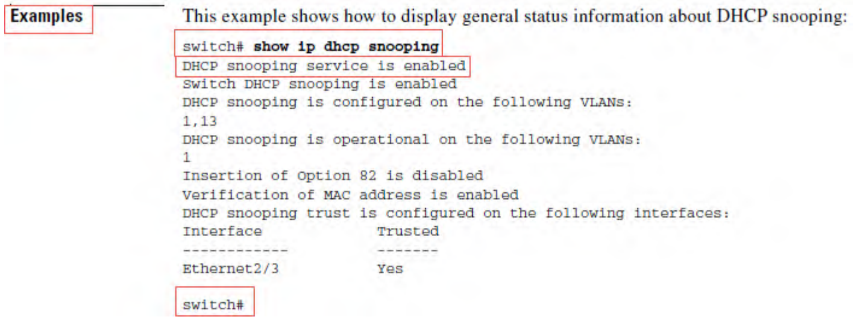
Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1237.

</td>
</tr>
<tr>
<td>

Cisco NX-OS 6.2

Effective date of registration: 11/13/2014

</td>
<td>

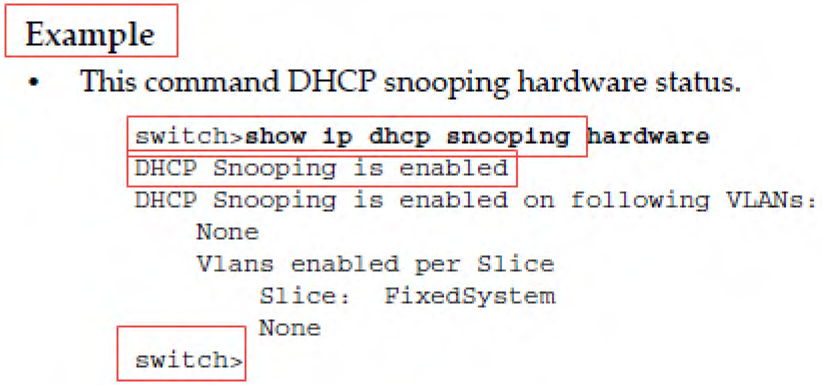


Examples This example shows how to display general status information about DHCP snooping:

```
switch# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
1,13
DHCP snooping is operational on the following VLANs:
1
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted
------------          -------
Ethernet2/3           Yes

switch#
```

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-634.

</td>
<td>



Example

- This command DHCP snooping hardware status.

```
switch>show ip dhcp snooping hardware
DHCP Snooping is enabled
DHCP Snooping is enabled on following VLANs:
    None
    Vlans enabled per Slice
        Slice:  FixedSystem
        None
switch>
```

Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1304.

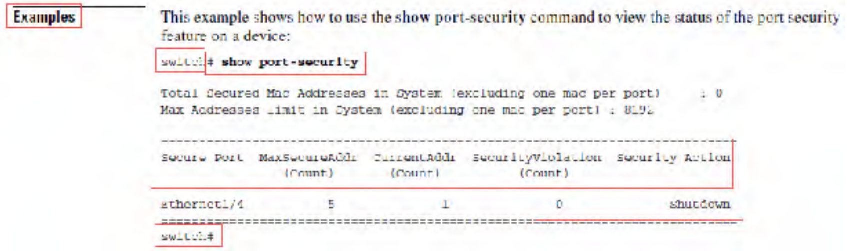
</td>
</tr>
</table>

<table>
<tr>
<th>Copyright Registration Information</th>
<th>Cisco</th>
<th>Arista</th>
</tr>
<tr>
<td>

Cisco NX-OS 6.2

Effective date of registration: 11/13/2014

</td>
<td>



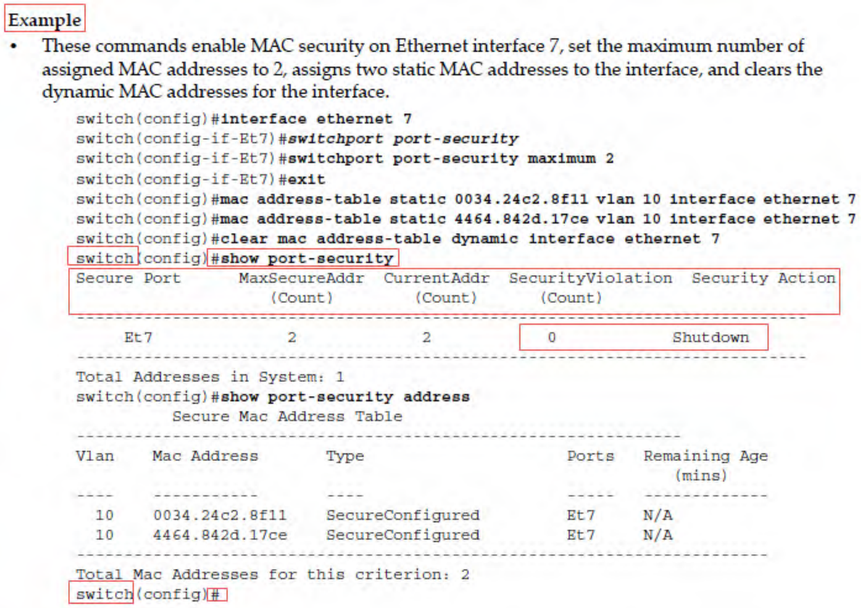
Examples

This example shows how to use the show port-security command to view the status of the port security feature on a device:

```
switch# show port-security

Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

----------------------------------------------------------------------------
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)         (Count)

ethernet1/4           5            1              0                shutdown
============================================================================
switch#
```

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-661.

</td>
<td>



Example

- These commands enable MAC security on Ethernet interface 7, set the maximum number of assigned MAC addresses to 2, assigns two static MAC addresses to the interface, and clears the dynamic MAC addresses for the interface.

```
switch(config)#interface ethernet 7
switch(config-if-Et7)#switchport port-security
switch(config-if-Et7)#switchport port-security maximum 2
switch(config-if-Et7)#exit
switch(config)#mac address-table static 0034.24c2.8f11 vlan 10 interface ethernet 7
switch(config)#mac address-table static 4464.842d.17ce vlan 10 interface ethernet 7
switch(config)#clear mac address-table dynamic interface ethernet 7
switch(config)#show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)       (Count)         (Count)
---------------------------------------------------------------------------
     Et7               2            2              0               Shutdown
---------------------------------------------------------------------------
Total Addresses in System: 1
switch(config)#show port-security address
              Secure Mac Address Table
-----------------------------------------------------------------------
Vlan     Mac Address        Type                    Ports    Remaining Age
                                                                (mins)
----     -----------        ----                    -----    -------------
  10     0034.24c2.8f11     SecureConfigured        Et7      N/A
  10     4464.842d.17ce     SecureConfigured        Et7      N/A
------------------------------------------------------------------------
Total Mac Addresses for this criterion: 2
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 632.

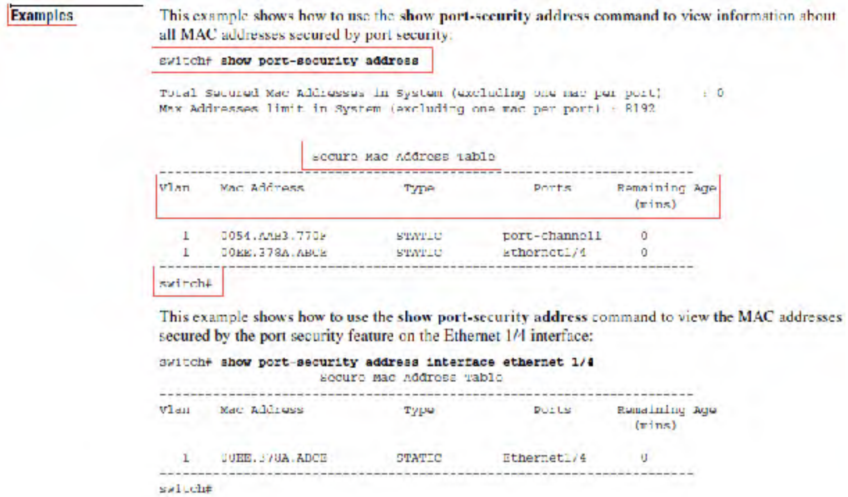
</td>
</tr>
</table>

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>

Cisco NX-OS 6.2

Effective date of registration: 11/13/2014

</td>
<td>



Examples This example shows how to use the **show port-security address** command to view information about all MAC addresses secured by port security:

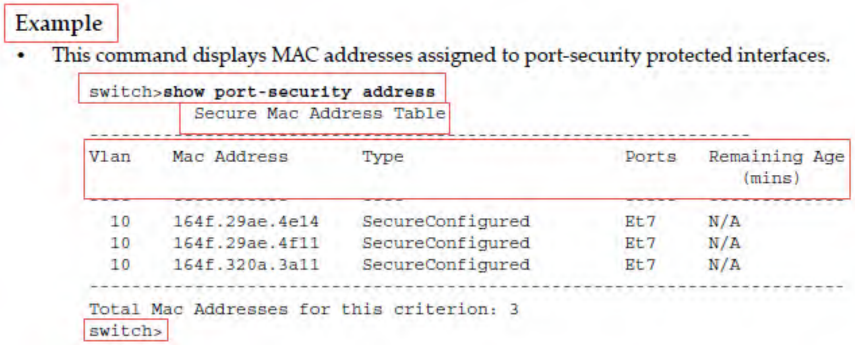
```
switch# show port-security address

Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

                    Secure Mac Address Table
----------------------------------------------------------------------
Vlan    Mac Address          Type          Ports          Remaining Age
                                                               (mins)

   1    0054.AAB3.770F       STATIC        port-channel1      0
   1    00EE.378A.ABCE       STATIC        ethernet1/4        0
----------------------------------------------------------------------
switch#
```

This example shows how to use the **show port-security address** command to view the MAC addresses secured by the port security feature on the Ethernet 1/4 interface:

```
switch# show port-security address interface ethernet 1/4
                    Secure Mac Address Table
----------------------------------------------------------------------
Vlan    Mac Address          Type          Ports          Remaining Age
                                                               (mins)

   1    00EE.378A.ABCE       STATIC        Ethernet1/4        0
----------------------------------------------------------------------
switch#
```

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-664.

</td>
<td>



Example

- This command displays MAC addresses assigned to port-security protected interfaces.

```
switch>show port-security address
          Secure Mac Address Table
---------------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports     Remaining Age
                                                            (mins)
----    -----------       ----                  -----     -------------
  10    164f.29ae.4e14    SecureConfigured      Et7       N/A
  10    164f.29ae.4f11    SecureConfigured      Et7       N/A
  10    164f.320a.3a11    SecureConfigured      Et7       N/A
---------------------------------------------------------------------------
Total Mac Addresses for this criterion: 3
switch>
```

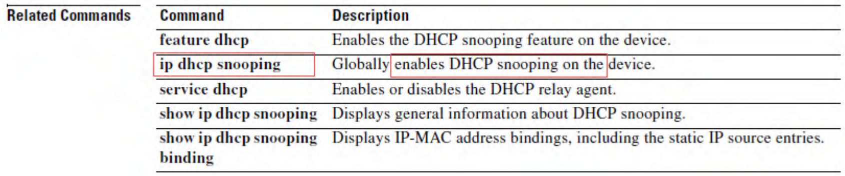
Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 698.

</td>
</tr>
<tr>
<td>

Cisco NX-OS 6.2

Effective date of registration: 11/13/2014

</td>
<td>

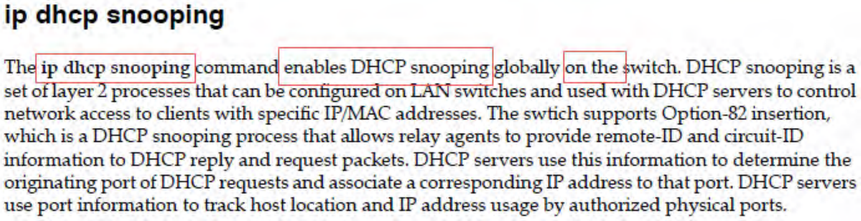


Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping	Globally enables DHCP snooping on the device.
service dhcp	Enables or disables the DHCP relay agent.
show ip dhcp snooping	Displays general information about DHCP snooping.
show ip dhcp snooping binding	Displays IP-MAC address bindings, including the static IP source entries.

Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-695.

</td>
<td>

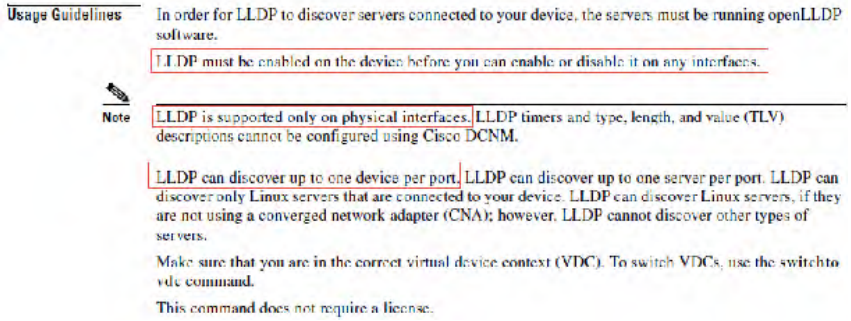
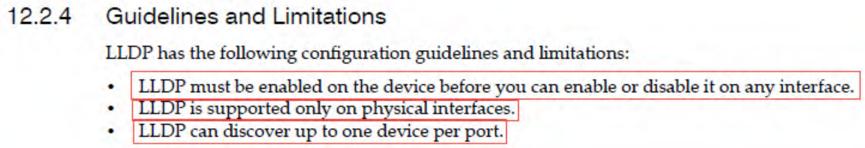


ip dhcp snooping

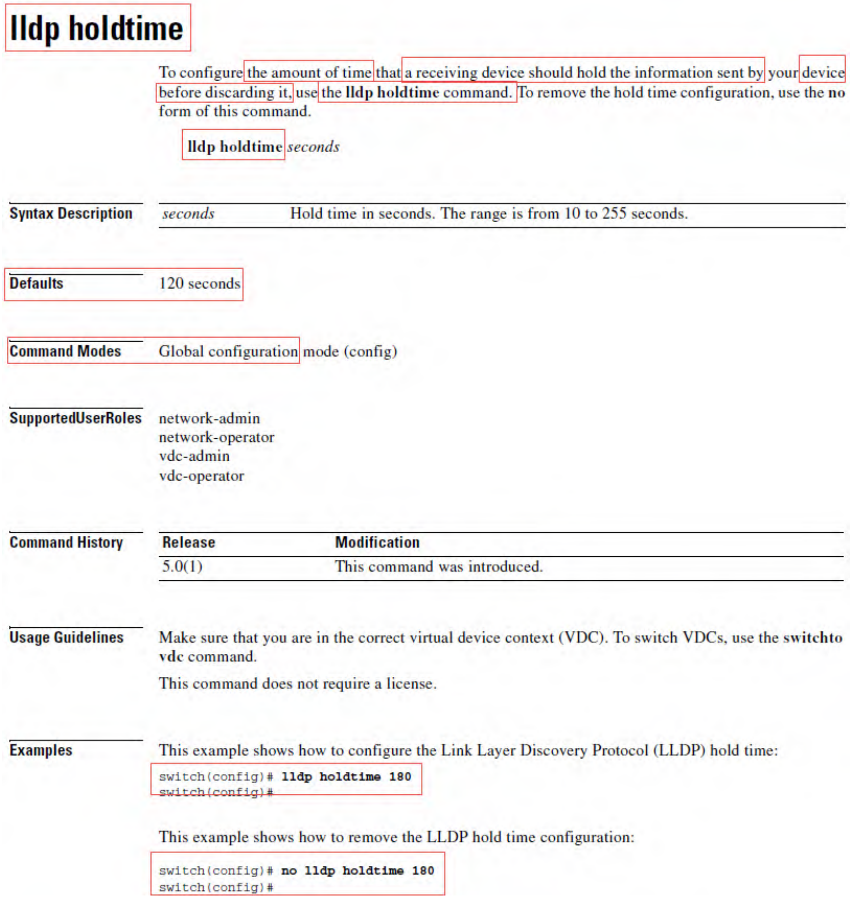
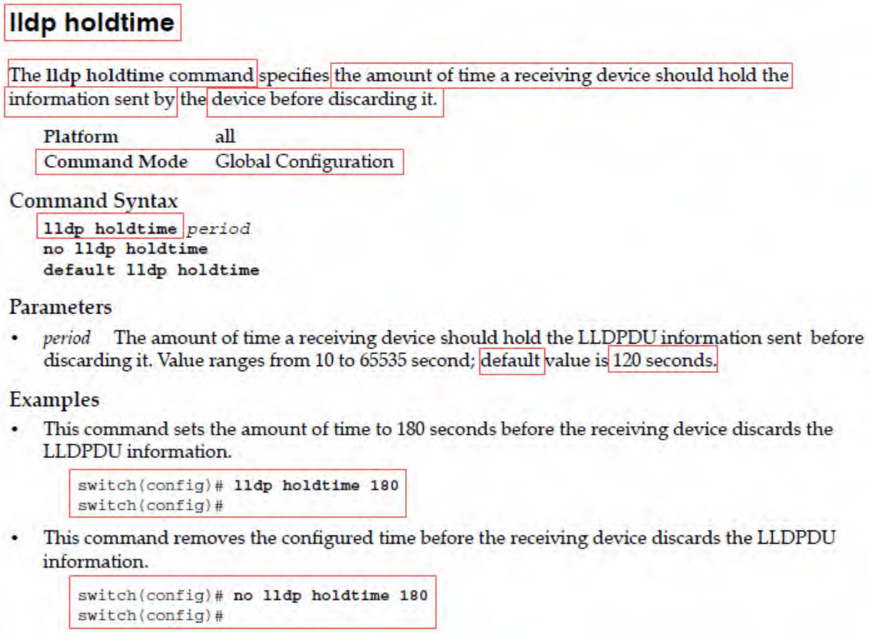
The **ip dhcp snooping** command enables DHCP snooping globally on the switch. DHCP snooping is a set of layer 2 processes that can be configured on LAN switches and used with DHCP servers to control network access to clients with specific IP/MAC addresses. The swtich supports Option-82 insertion, which is a DHCP snooping process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP servers use port information to track host location and IP address usage by authorized physical ports.

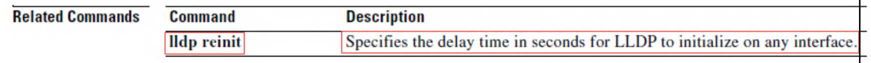
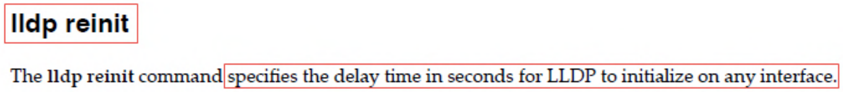
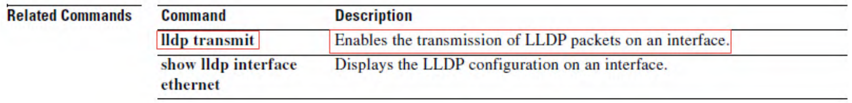
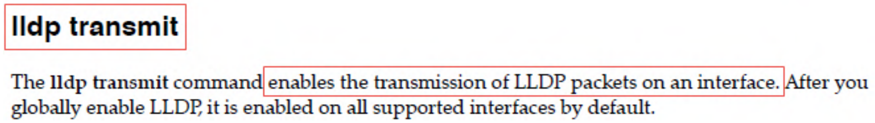
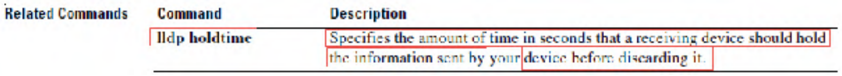
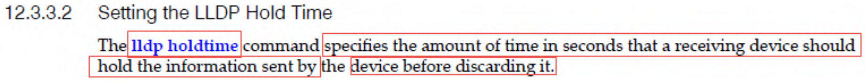
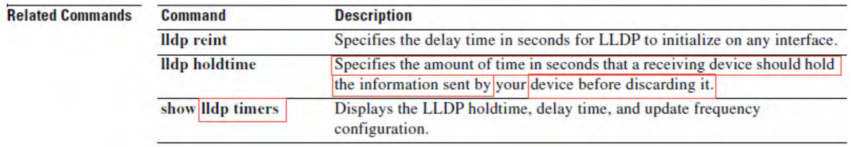
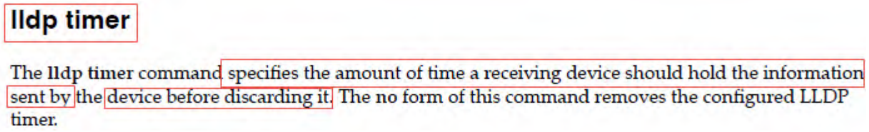
Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1269.

</td>
</tr>
</table>

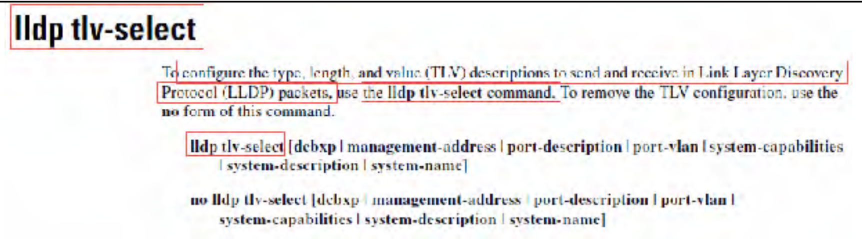
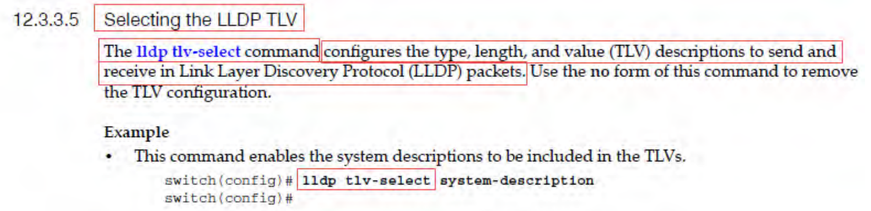
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Usage Guidelines** In order for LLDP to discover servers connected to your device, the servers must be running openLLDP software. LLDP must be enabled on the device before you can enable or disable it on any interfaces. Note LLDP is supported only on physical interfaces. LLDP timers and type, length, and value (TLV) descriptions cannot be configured using Cisco DCNM. LLDP can discover up to one device per port. LLDP can discover up to one server per port. LLDP can discover only Linux servers that are connected to your device. LLDP can discover Linux servers, if they are not using a converged network adapter (CNA); however, LLDP cannot discover other types of servers. Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the switchto vdc command. This command does not require a license. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 174.	 12.2.4 Guidelines and Limitations LLDP has the following configuration guidelines and limitations: • LLDP must be enabled on the device before you can enable or disable it on any interface. • LLDP is supported only on physical interfaces. • LLDP can discover up to one device per port. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 576.

Copyright Registration Information	Cisco	Arista

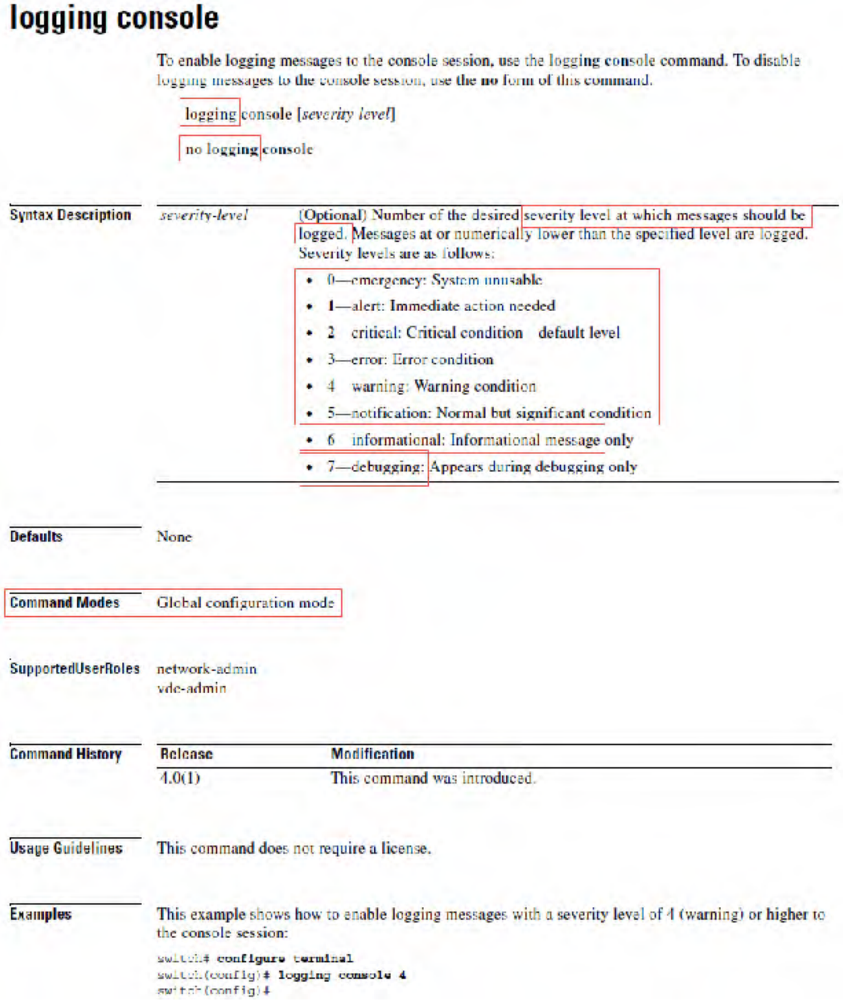
Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	lldp holdtime
	To configure the amount of time that a receiving device should hold the information sent by your device before discarding it, use the **lldp holdtime** command. To remove the hold time configuration, use the no form of this command.
	lldp holdtime *seconds*
	Syntax Description — *seconds* — Hold time in seconds. The range is from 10 to 255 seconds.
	Defaults — 120 seconds
	Command Modes — Global configuration mode (config)
	SupportedUserRoles — network-admin
	network-operator
	vdc-admin
	vdc-operator
	Command History — **Release** — **Modification**
	5.0(1) — This command was introduced.
	Usage Guidelines — Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the **switchto vdc** command.
	This command does not require a license.
	Examples — This example shows how to configure the Link Layer Discovery Protocol (LLDP) hold time:
	`switch(config)# lldp holdtime 180`
	`switch(config)#`
	This example shows how to remove the LLDP hold time configuration:
	`switch(config)# no lldp holdtime 180`
	`switch(config)#`
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 228.
		
		lldp holdtime
		The **lldp holdtime** command specifies the amount of time a receiving device should hold the information sent by the device before discarding it.
		Platform — all
		Command Mode — Global Configuration
		Command Syntax
		`lldp holdtime` *`period`*
		`no lldp holdtime`
		`default lldp holdtime`
		Parameters
		- *period* The amount of time a receiving device should hold the LLDPDU information sent before discarding it. Value ranges from 10 to 65535 second; default value is 120 seconds.
		Examples
		- This command sets the amount of time to 180 seconds before the receiving device discards the LLDPDU information.
		`switch(config)# lldp holdtime 180`
		`switch(config)#`
		- This command removes the configured time before the receiving device discards the LLDPDU information.
		`switch(config)# no lldp holdtime 180`
		`switch(config)#`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 585.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands — Command: Description lldp reinit: Specifies the delay time in seconds for LLDP to initialize on any interface. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 228.	 **lldp reinit** The **lldp reinit** command specifies the delay time in seconds for LLDP to initialize on any interface. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 589.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands — Command: Description lldp transmit: Enables the transmission of LLDP packets on an interface. show lldp interface ethernet: Displays the LLDP configuration on an interface. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 231.	 **lldp transmit** The **lldp transmit** command enables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 593.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands — Command: Description lldp holdtime: Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 232.	 12.3.3.2 Setting the LLDP Hold Time The **lldp holdtime** command specifies the amount of time in seconds that a receiving device should hold the information sent by the device before discarding it. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 578.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands — Command: Description lldp reint: Specifies the delay time in seconds for LLDP to initialize on any interface. lldp holdtime: Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it. show lldp timers: Displays the LLDP holdtime, delay time, and update frequency configuration. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 235.	 **lldp timer** The **lldp timer** command specifies the amount of time a receiving device should hold the information sent by the device before discarding it. The no form of this command removes the configured LLDP timer. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 591.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	lldp tlv-select
	To configure the type, length, and value (TLV) descriptions to send and receive in Link Layer Discovery Protocol (LLDP) packets, use the **lldp tlv-select** command. To remove the TLV configuration, use the **no** form of this command.
	lldp tlv-select [**dcbxp** | **management-address** | **port-description** | **port-vlan** | **system-capabilities** | **system-description** | **system-name**]
	no lldp tlv-select [**dcbxp** | **management-address** | **port-description** | **port-vlan** | **system-capabilities** | **system-description** | **system-name**]
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 236.
		
		12.3.3.5 Selecting the LLDP TLV
		The **lldp tlv-select** command configures the type, length, and value (TLV) descriptions to send and receive in Link Layer Discovery Protocol (LLDP) packets. Use the no form of this command to remove the TLV configuration.
		Example
		- This command enables the system descriptions to be included in the TLVs.
		`switch(config)# lldp tlv-select system-description`
		`switch(config)#`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 578.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 6.2
Effective date of registration: 11/13/2014</td>
<td>



logging console

To enable logging messages to the console session, use the **logging console** command. To disable logging messages to the console session, use the **no** form of this command.

logging console [*severity level*]

no logging console

Syntax Description

severity-level (Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:

- 0—emergency: System unusable
- 1—alert: Immediate action needed
- 2 critical: Critical condition default level
- 3—error: Error condition
- 4 warning: Warning condition
- 5—notification: Normal but significant condition
- 6 informational: Informational message only
- 7—debugging: Appears during debugging only

Defaults None

Command Modes Global configuration mode

SupportedUserRoles network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

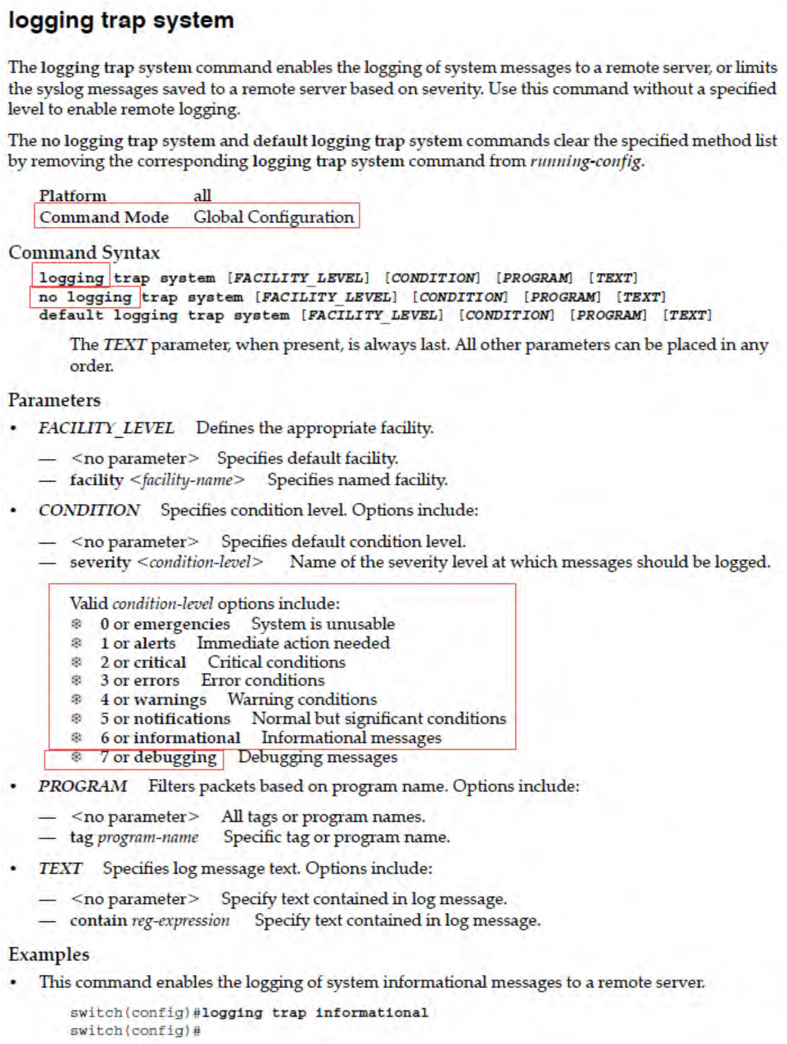
Usage Guidelines This command does not require a license.

Examples This example shows how to enable logging messages with a severity level of 4 (warning) or higher to the console session:

```
switch# configure terminal
switch(config)# logging console 4
switch(config)#
```

Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 242.

</td>
<td>



logging trap system

The logging trap system command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging.

The no logging trap system and default logging trap system commands clear the specified method list by removing the corresponding logging trap system command from *running-config*.

Platform	all
Command Mode	Global Configuration

Command Syntax

```
logging trap system [FACILITY_LEVEL] [CONDITION] [PROGRAM] [TEXT]
no logging trap system [FACILITY_LEVEL] [CONDITION] [PROGRAM] [TEXT]
default logging trap system [FACILITY_LEVEL] [CONDITION] [PROGRAM] [TEXT]
```

The *TEXT* parameter, when present, is always last. All other parameters can be placed in any order.

Parameters

- *FACILITY_LEVEL* Defines the appropriate facility.
  - — <no parameter> Specifies default facility.
  - — facility <*facility-name*> Specifies named facility.
- *CONDITION* Specifies condition level. Options include:
  - — <no parameter> Specifies default condition level.
  - — severity <*condition-level*> Name of the severity level at which messages should be logged.

Valid *condition-level* options include:

0 or emergencies	System is unusable
1 or alerts	Immediate action needed
2 or critical	Critical conditions
3 or errors	Error conditions
4 or warnings	Warning conditions
5 or notifications	Normal but significant conditions
6 or informational	Informational messages
7 or debugging	Debugging messages

- *PROGRAM* Filters packets based on program name. Options include:
  - — <no parameter> All tags or program names.
  - — tag *program-name* Specific tag or program name.
- *TEXT* Specifies log message text. Options include:
  - — <no parameter> Specify text contained in log message.
  - — contain *reg-expression* Specify text contained in log message.

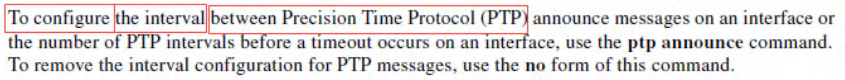
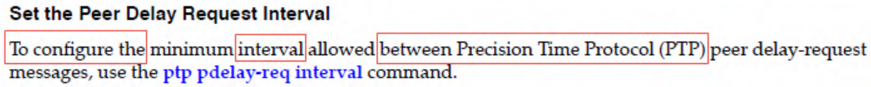
Examples

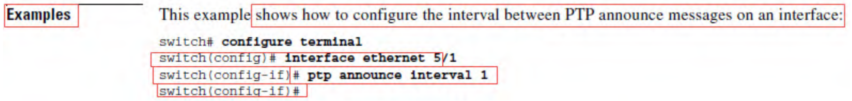
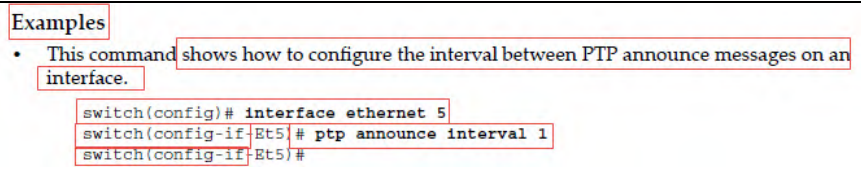
- This command enables the logging of system informational messages to a remote server.

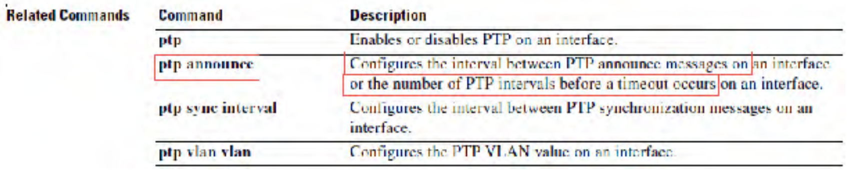
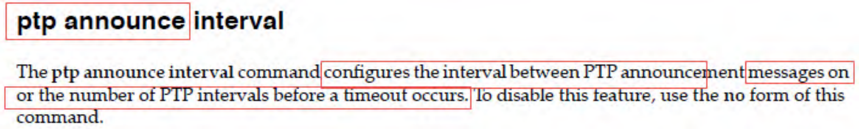
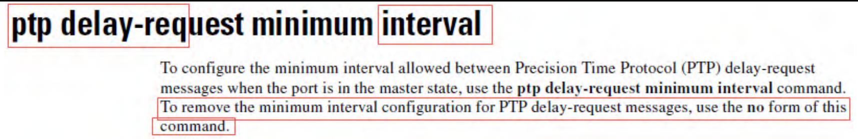
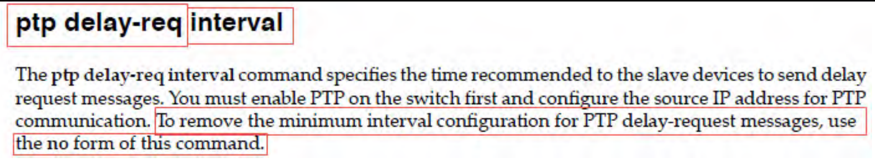
```
switch(config)#logging trap informational
switch(config)#
```

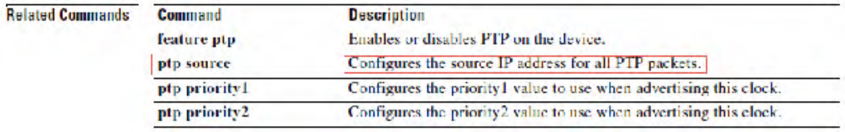
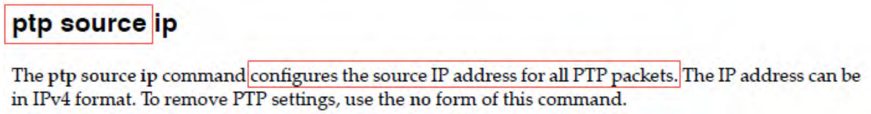
Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 155.

</td>
</tr>
</table>

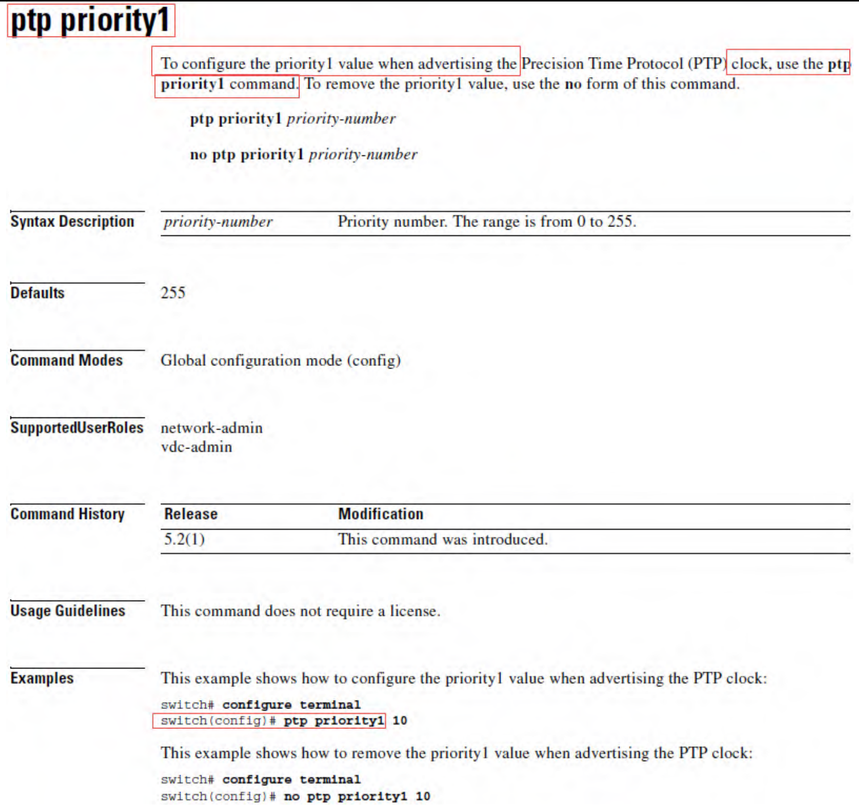
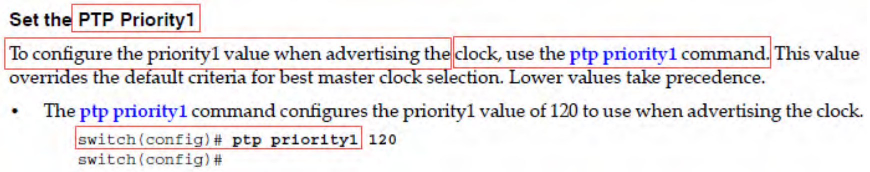
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 To configure the interval between Precision Time Protocol (PTP) announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface, use the **ptp announce** command. To remove the interval configuration for PTP messages, use the **no** form of this command. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 330.	 **Set the Peer Delay Request Interval** To configure the minimum interval allowed between Precision Time Protocol (PTP) peer delay-request messages, use the **ptp pdelay-req interval** command. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 273.

Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	Examples This example shows how to configure the interval between PTP announce messages on an interface:
	`switch# configure terminal`
	`switch(config)# interface ethernet 5/1`
	`switch(config-if)# ptp announce interval 1`
	`switch(config-if)#`
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 330.
		
		Examples
		• This command shows how to configure the interval between PTP announce messages on an interface.
		`switch(config)# interface ethernet 5`
		`switch(config-if-Et5)# ptp announce interval 1`
		`switch(config-if-Et5)#`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 315.

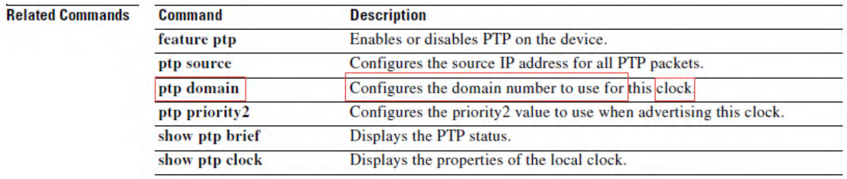
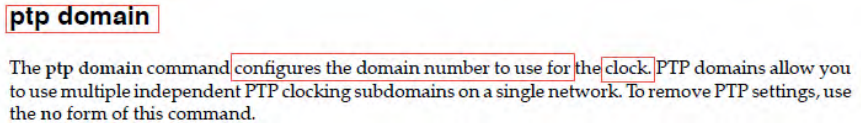
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Related Commands** **Command** — **Description** **ptp** — Enables or disables PTP on an interface. **ptp announce** — Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface. **ptp sync interval** — Configures the interval between PTP synchronization messages on an interface. **ptp vlan vlan** — Configures the PTP VLAN value on an interface. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 333.	 **ptp announce interval** The ptp announce interval command configures the interval between PTP announcement messages on or the number of PTP intervals before a timeout occurs. To disable this feature, use the no form of this command. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 315.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **ptp delay-request minimum interval** To configure the minimum interval allowed between Precision Time Protocol (PTP) delay-request messages when the port is in the master state, use the **ptp delay-request minimum interval** command. To remove the minimum interval configuration for PTP delay-request messages, use the **no** form of this command. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 332.	 **ptp delay-req interval** The **ptp delay-req interval** command specifies the time recommended to the slave devices to send delay request messages. You must enable PTP on the switch first and configure the source IP address for PTP communication. To remove the minimum interval configuration for PTP delay-request messages, use the no form of this command. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 318.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands Command — Description feature ptp — Enables or disables PTP on the device. ptp source — Configures the source IP address for all PTP packets. ptp priority1 — Configures the priority1 value to use when advertising this clock. ptp priority2 — Configures the priority2 value to use when advertising this clock. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 334.	 ptp source ip The ptp source ip command configures the source IP address for all PTP packets. The IP address can be in IPv4 format. To remove PTP settings, use the no form of this command. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 328.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	ptp priority1
	To configure the priority1 value when advertising the Precision Time Protocol (PTP) clock, use the **ptp priority1** command. To remove the priority1 value, use the **no** form of this command.
	ptp priority1 *priority-number*
	no ptp priority1 *priority-number*
	Syntax Description — *priority-number*: Priority number. The range is from 0 to 255.
	Defaults — 255
	Command Modes — Global configuration mode (config)
	SupportedUserRoles — network-admin
	vdc-admin
	Command History — **Release**: 5.2(1); **Modification**: This command was introduced.
	Usage Guidelines — This command does not require a license.
	Examples — This example shows how to configure the priority1 value when advertising the PTP clock:
	`switch# configure terminal`
	`switch(config)# ptp priority1 10`
	This example shows how to remove the priority1 value when advertising the PTP clock:
	`switch# configure terminal`
	`switch(config)# no ptp priority1 10`
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 336.
		
		Set the PTP Priority1
		To configure the priority1 value when advertising the clock, use the ptp priority1 command. This value overrides the default criteria for best master clock selection. Lower values take precedence.
		• The ptp priority1 command configures the priority1 value of 120 to use when advertising the clock.
		`switch(config)# ptp priority1 120`
		`switch(config)#`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 272.

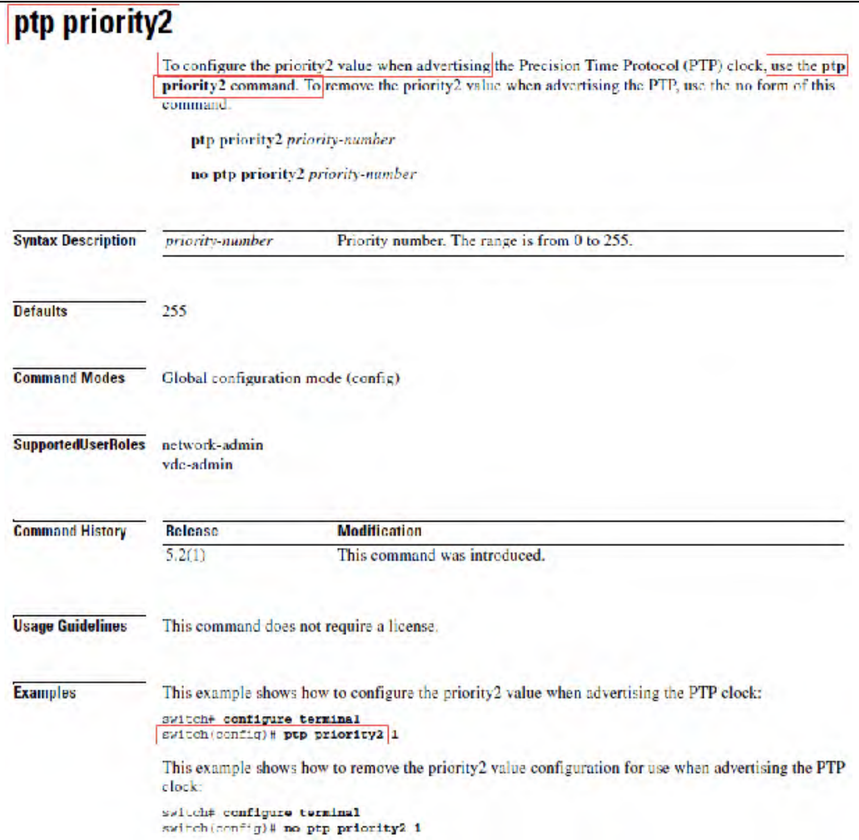
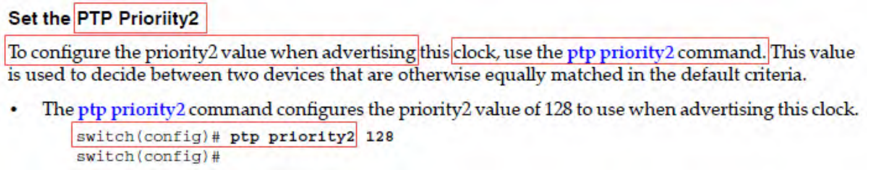
<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr>
<td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td>
<td>
<table>
<tr><th>Related Commands</th><th>Command</th><th>Description</th></tr>
<tr><td></td><td><b>feature ptp</b></td><td>Enables or disables PTP on the device.</td></tr>
<tr><td></td><td><b>ptp source</b></td><td>Configures the source IP address for all PTP packets.</td></tr>
<tr><td></td><td><b>ptp domain</b></td><td>Configures the domain number to use for this clock</td></tr>
<tr><td></td><td><b>ptp priority2</b></td><td>Configures the priority2 value to use when advertising this clock.</td></tr>
<tr><td></td><td><b>show ptp brief</b></td><td>Displays the PTP status.</td></tr>
<tr><td></td><td><b>show ptp clock</b></td><td>Displays the properties of the local clock.</td></tr>
</table>
Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 336.</td>
<td>
<b>ptp domain</b>

The <b>ptp domain</b> command configures the domain number to use for the clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. To remove PTP settings, use the <b>no</b> form of this command.

Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 319.</td>
</tr>
</table>

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
Effective date of registration: 11/13/2014
	
	ptp priority2
	To configure the priority2 value when advertising the Precision Time Protocol (PTP) clock, use the **ptp priority2** command. To remove the priority2 value when advertising the PTP, use the **no** form of this command.
	ptp priority2 *priority-number*
	no ptp priority2 *priority-number*
	Syntax Description *priority-number* Priority number. The range is from 0 to 255.
	Defaults 255
	Command Modes Global configuration mode (config)
	SupportedUserRoles network-admin
	vdc-admin
	Command History **Release** **Modification**
	5.2(1) This command was introduced.
	Usage Guidelines This command does not require a license.
	Examples This example shows how to configure the priority2 value when advertising the PTP clock:
	`switch# configure terminal`
	`switch(config)# ptp priority2 1`
	This example shows how to remove the priority2 value configuration for use when advertising the PTP clock:
	`switch# configure terminal`
	`switch(config)# no ptp priority2 1`
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 337.
		
		Set the PTP Prioriity2
		To configure the priority2 value when advertising this clock, use the ptp priority2 command. This value is used to decide between two devices that are otherwise equally matched in the default criteria.
		- The ptp priority2 command configures the priority2 value of 128 to use when advertising this clock.
		`switch(config)# ptp priority2 128`
		`switch(config)#`
		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 272.